LOW LATENCY MOBILE INITIATED TUNNELING HANDOFF

Patent number: JP2003209872 (A)

Publication date: 2003-07-25

Inventor(s): GWON YOUNGJUNE L; KEMPF JAMES; FUNATO DAICHI; TAKESHITA ATSUSHI

Applicant(s): DOCOMO COMM LAB USA INC

Classification:

- international: ***H04L12/56; H04W36/14;*** *H04W36/02; H04W36/12; H04W80/04;* **H04L12/56; H04W36/00;** H04W80/00; (IPC1-7): H04Q7/22; H04L12/56; H04Q7/28

- european: H04W36/14; H04L12/56B; H04Q7/38H

Application number: JP20020348438 20021129

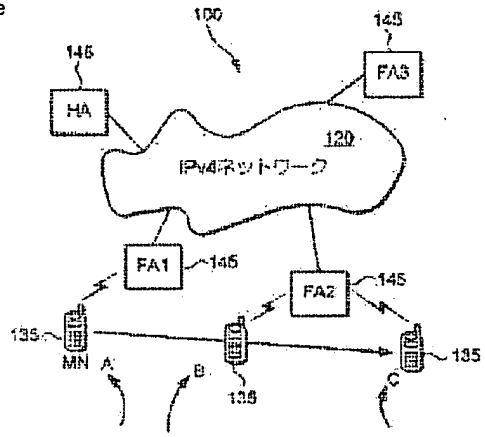
Priority number(s): US20010334481P 20011130; US20020138389 20020503

Also published as:

US2003104814 (A1)

Abstract of **JP 2003209872 (A)**

PROBLEM TO BE SOLVED: To provide a tunnel-based IP handoff process that can minimize the handoff latency. ; SOLUTION: Tunnels are established between two mobility service providing nodes (source node and target node). The tunnels are used for communication between the mobile node and the source node after the mobile node performs L2 handoff from the source node to the target node and before a standard mobile IP registration process (that is, update of IP routing) with respect to the target node. The tunnels may be established before or after the mobile node performs the L2 handoff from the source node to the source node to the target node. Further, the tunnels may be established by a trigger produced inside or outside of the mobile node. ; COPYRIGHT: (C)2003,JPO



Data supplied from the *esp@cenet* database — Worldwide

LOW LATENCY MOBILE INITIATED TUNNELING HANDOFF

Description of correspondent: **US 2003104814 (A1)**

[0001] This application claims the benefit of U.S. Provisional Application No. 60/334,481, filed Nov. 30, 2001, and titled "Low Latency Mobile Triggered Post Registration Tunneling Handoff Scheme for Mobile IPv4 and Mobile IPv6," which is incorporated herein by reference.

FIELD OF THE INVENTION

[0002] This invention relates generally to the communication of digital data in digital data networks and more specifically to communication of digital data in wireless, mobile-access, Internet protocol-based data networks. This invention is particularly relevant to real-time interactive digital data communications such as voice over Internet protocol (VoIP) and real time interactive multi-media.

BACKGROUND OF THE INVENTION

[0003] The need for personal wireless communications is expanding rapidly with the advances in digital communications and personal communications systems. The progress in cellular radio technology and the growth rate of the cellular telephone systems over the last several years is indicative of tremendous market demand for location independent communication via wireless access. Wireless or mobile cellular communications systems have evolved through generational changes since the first generation (1 G) wireless communications systems were first deployed commercially about two decades ago. The 1 G systems were entirely analog and primarily used for voice communication. Currently, the third generation (3 G) wireless communications systems are being introduced. The third generation (3 G) is defined by the ITU under the IMT-2000 global framework and is implemented by new communication technologies, such as W-CDMA and CDMA2000. 3 G is designed for high-speed multimedia data and voice, and its goals include high-quality audio and video and advanced global roaming, which means being able to go anywhere and automatically be handed off to whatever wireless system is available (in-house phone system, cellular, satellite, etc.). Unlike previous wireless communications systems, 3 G systems, depending on their system architectures, may be entirely IP based, i.e., all data is communicated in digital form via standard Internet addressing and routing protocols from end to end.

[0004] Most of the functionality in the OSI model also exists in wireless IP communication. The OSI multi-layer model defines 7-layer communication protocols. For example, the OSI model specifies a hierarchy of protocols including low level physical hardware specifications and connections (Layer 1), radio data link establishment and format (Layer 2), IP network addressing and routing (Layer 3) data transport rules (Layer 4), Session (Layer 5), Presentation (Layer 6) and Application (Layer 7). The Layer 2 is responsible for radio link between nodes and implements specific radio access technology. The Layer 3, which is sometimes referred to as the IP layer, performs routing of packets or IP datagrams.

[0005] Throughout evolution of wireless communications systems, technical challenges associated with implementing wireless communication have always been posed by a mobile node (MN), as traveling from one area to another, irregularly changing its point of attachment to terrestrial radio access point (AP) with which it is communicating wirelessly. Indeed, the most critical factor in achieving good performance for mobility protocols is the design of handoff. A handoff occurs when a MN moves from one radio AP to another. A mere change of radio AP is called a "Layer 2 (L2) handoff," which does not involve any Layer 3 (L3) signaling at the IP level. If the new radio access point is associated with a new subnet, i.e., if the MN moves from one subnet to another, a changing in routing reachability occurs and requires Layer 3 (L3) protocol action. This L3 protocol action is called a "L3 handoff" and usually involves exchange of a series of IP messages that are used to update routing information for the MN to make sure that data destined to the MN is routed through the new subnet to the MN.

[0006] The Internet Engineering Task Force (IETF) has proposed several standards to deal with the handoff operations. For instance, IETF RFC 2002 titled "IP Mobility Support," which is usually referred to as Mobile IP Version 4 (IPv4) and incorporated herein by reference, describes how a MN can perform L3 handoffs between subnets served by different agents. Under IPv4, a MN is given a long-term home address by its home agent (HA) and uses the home address as the source address of all IP data that it sends. When located on a foreign subnet away from its home subnet, a "care-of address" (CoA) is associated with the MN and reflects the MN's current point of attachment. Through an L3 handoff, the CoA is registered in the MN's home agent to enable the HA to update its binding or data-routing information for the MN.

[0007] The L3 handoff process pursuant to RFC 2002 requires mobility agents, i.e., foreign agents and home agents, to advertise their presence via Agent Advertisement messages. A MN that receives these Agent Advertisements determines whether it is operating on its home subnet or a foreign subnet. When the MN detects that it has entered a new subnet, it obtains a CoA from Agents Advertisements sent from the foreign agent serving the foreign network. The MN then registers the new CoA by sending a registration request including the CoA to its home agent (HA). The L3 handoff completes when the HA receiving the registration request updates its internal binding information for the MN and returns a registration reply to the MN. After the registration, data sent to the MN's home address are intercepted by the HA, tunneled by the same to the MN's CoA, received at the tunnel endpoint (either at a FA or at the MN itself), and finally delivered to the MN. In the reverse direction, data sent by the MN is generally delivered to its destination using standard IP routing mechanisms, not necessarily passing through the HA.

[0008] Mobile IP was originally designed without any assumptions about the underlying link layers over which it would operate so that it could have the widest possible applicability. This approach has the advantage of facilitating a clean separation between L2 and L3 of the protocol stack, but it has negative consequences. Because of the strict separation between L2 and L3, a MN may only communicate with a directly connected FA. This implies that a MN may not begin the registration process until it obtains L2 connectivity to a new FA after having lost L2 connectivity to the old or previous FA. In addition, the registration process itself takes some time to complete as the registration request and reply messages propagate through networks between the MN to its HA. The time from the last L3 connectivity between the MN and the old FA, to the time when the L3 connectivity to the new FA has been established manifests itself as handoff latency. During this time period, the MN is not able to send or receive any data. The handoff latency resulting from standard Mobile IP handoff procedures could be greater than what is acceptable to support real-time or delay sensitive traffic.

[0009] Several protocol designs have been proposed for both Mobile IPv4 and IPv6 that seek to reduce the amount of handoff latency. For instance, Internet Draft "Low Latency Handoffs in Mobile IPv4" <draft-ietf-mobileip-lowlatency-handoffs-v4-03.txt>, which is incorporated herein by reference, proposes two techniques for minimizing the period of time when a MN is unable to send or receive data due to the delay in the Mobile IP registration process. One such technique

is "pre-registration handoff" which allows the MN to communicate with a new FA while still connected to the old FA. The other is called "post-registration handoff" which provides for data delivery to the MN at the new FA even before the formal registration process has completed. More specifically, under the pre-registration handoff method, the old FA, initiated by an L2 trigger, notifies the MN of a new FA. The MN then begins an L3 handoff with the new FA while still in communication with the old FA, i.e., while receiving and sending data through the old FA. In other words, the pre-registration handoff method allows the L3 handoff to begin even before the L2 handoff begins and thus helps achieve seamless handoffs between old and new FAs. The new FA may initiate the pre-registration handoff by sending its presence through the old FA to the MN. Also, the MN may become an initiator of the pre-registration handoff by sending a Proxy Router Solicitation to the old FA, which in return advises the MN of the new FA. In any event, a prompt and timely L2 trigger is necessary to implement the pre-registration handoff.

[0010] The post-registration handoff method allows the old FA and new FA to utilize L2 triggers to set up a bi-directional tunnel (BDT) between the old FA and new FA that allows the MN to continue using the old FA while on the new FA's subnet. The post-registration handoff is likewise initiated by an L2 trigger that is provided to either the old FA or the new FA. Following a successful Mobile IP Registration between the MN and the old FA, the old FA becomes the mobility anchor point for the MN. Either the old FA or the new FA then receives an L2 trigger informing that the MN is about to move from the old FA to the new FA. The FA (old or new FA) receiving the trigger sends a Handoff Request to the other FA (new or old FA), which returns a Handoff Reply, thereby creating a bidirectional tunnel between the FAs. When the link between old FA and MN is disconnected, the old FA begins forwarding MN-bound data through the tunnel to the new FA. When a new link is established between new FA and MN, the new FA begins delivering the data tunneled from the old FA to the MN and forwards any data from the MN through the reverse tunnel to the old FA. After the L2 handoff is completed, the MN may, while sending and receiving data through the tunnel from the new FA, perform a formal Mobile IP registration with the new FA. The initiation of this formal registration may be delayed. Thus, the post-registration handoff enables a rapid establishment of service at the new FA.

[0011] Internet Draft "Fast Handovers for Mobile Ipv6" <draft-ietf-mobileip-fast-mipv6-03.txt>, which is incorporated herein by reference, proposes similar techniques for minimizing the handoff latency for Mobile Ipv6.

[0012] In both pre and post-registration handoff methods, it is assumed that L2 triggers are properly fired at right timings. An L2 trigger is an abstraction of a notification from L2 that a certain event related to the L2 handoff process has happened or is about to happen. One possible event is early notice of an upcoming change in the L2 point of attachment of the MN. Other possible events are disconnection of the MN's point of attachment from the old L2 access point and establishment of the MN's point of attachment to a new L2 access point. Usually, firing of L2 triggers is assisted by a radio access network (RAN) or radio network controller (RNC) located in a subnetwork, which keeps track of and maintains location information of all the MNs situated within the subnetwork. Accordingly, prompt and timely firing of L2 triggers necessitates close collaboration of two neighboring RANs over which the MN is traveling. Since close collaboration by two RANs is possible only when they support the same radio access technology, the above assumption regarding the L2 trigger firing may practically be translated into an assumption that two neighboring RANs over which the MN is traveling support the same radio access technology. However, current trends in wireless networking suggest that future wireless networks will consist of a variety heterogeneous RANs that support different radio access technologies. The proposed pre and post-handoff protocols simply do not support such heterogeneous handoffs.

BRIEF SUMMARY OF THE INVENTION

[0013] The present invention provides a tunneling handoff process that can minimize the handoff latency associated with the standard Mobile IP registration. The invention is applicable in both Mobile IPv4 and IPv6. Thus, in this application, the term "agent" used in Mobile IPv4 and the term "router" or "access router" used in Mobile IPv6 may be used interchangeably with each other or collectively referred to as "mobility serving nodes."

[0014] The present invention contemplates a situation where a mobile node is leaving one subnet operated by one mobility serving node (source) and entering another subnet operated by another mobility serving node (target). In one embodiment according to the present invention, the mobile node, upon triggered, initiates the tunneling handoff process according to the present invention to establish a tunnel between the two mobility serving nodes, i.e., source and target nodes. After the mobile node has entered the new subnet operated by the target node, the standard Mobile IP registration process is delayed. Instead, the mobile node uses the tunnel to communicate with the source node while on the subnet operated by the target node. More specifically, in the present invention, the tunnel established between the source and target nodes will be used by the mobile node to communicate with the source node after the mobile node completes an L2 handoff from the source node to the target node but before completing an L3 handoff or undergoing IP routing update with the target node. The tunnel may be established either before or after the mobile node completes the L2 handoff between the source and target nodes.

[0015] In one embodiment, a mobile node is an entity that, upon triggered, performs initiation of the tunneling handoff process according to the present invention. The trigger is generated either externally or internally of the mobile node. Alternatively, the mobile node may use its internal L2 or L3 signaling to initiate the handoff process of the present invention. The mobile node can initiate the tunneling handoff scheme according the present invention irrespective of whether the source and target nodes support the same radio access technology or different radio access technologies.

[0016] In another embodiment, the mobile node, upon triggered, sends a tunneling handoff request to the source node to establish a tunnel before the mobile node initiates an L2 handoff from the source node to the target node. The mobile node obtains an L2 identifier, such as an L2 address, of the target node and includes the L2 identifier in the tunneling handoff request. The source node may in advance create a table containing L3 identifiers, such as L3 addresses or IP addresses, of neighboring networks in relation to their L2 identifiers and look up the table for the L3 identifier that corresponds to the L2 identifier in the tunneling handoff request from the mobile node. The mobile node may, if possible, obtain an L3 identifier of the target node and includes the L3 identifier in the tunneling handoff request.

[0017] Alternatively, the mobile node may send a tunneling handoff request to the target node to establish the tunnel after the mobile node completes an L2 handoff from the source node to the target node.

[0018] In another embodiment, in handoffs between source and target nodes that support different radio access technologies, any one of the mobile node, the source node and the target node may initiate the tunneling handoff process according to the present invention.

BRIEF DESCRIPTION OF THE DRAWINGS

[0019] FIG. 1 is a graphical representation of a third generation wireless, mobile access, IP data network in which the present invention is intended to operate;

[0020] FIG. 2 is a simplified graphical representation of the standard Mobile IP registration process;

[0021] FIG. 3a is a graphical representation illustrating a Pre-L2 handoff Mobile Initiated Tunneling Handoff (Pre-MIT) for

IPv4 according to an embodiment of the present invention;
[0022] FIG. 3b is a diagram illustrating trigger mode timing analysis for the Pre-MIT shown in FIG. 3a;
[0023] FIG. 3c is a diagram illustrating triggerless mode timing analysis for the Pre-MIT shown in FIG. 3a;
[0024] FIG. 4a is a graphical representation illustrating a Post-L2 handoff Mobile Initiated Tunneling Handoff (Post-MIT) for IPv4 according to another embodiment of the present invention;
[0025] FIG. 4b is a diagram illustrating trigger mode timing analysis for the Post-MIT shown in FIG. 4a;
[0026] FIG. 4c is a diagram illustrating triggerless mode timing analysis for the Post-MIT shown in FIG. 4a;
[0027] FIG. 5 is a graphical representation illustrating an agent solicitation message format used in an embodiment of the present invention;
[0028] FIG. 6 is a graphical representation illustrating an MIT request message format used in an embodiment of the present invention;
[0029] FIG. 7a is a graphical representation illustrating a Pre-MIT for IPv6 according to another embodiment of the present invention;
[0030] FIG. 7b is a diagram illustrating timing analysis for the Pre-MIT shown in FIG. 7a;
[0031] FIG. 8a is a graphical representation illustrating a Post-MIT for IPv6 according to another embodiment of the present invention;
[0032] FIG. 8b is a diagram illustrating timing analysis for the Post-MIT shown in FIG. 8a;
[0033] FIG. 9 is a graphical representation illustrating a mobile handoff initiation message format used in an embodiment of the present invention;
[0034] FIG. 10 is a graphical representation illustrating a source or target handoff initiation message format used in an embodiment of the present invention; and
[0035] FIG. 11 is a graphical representation illustrating a handoff acknowledgement message format used in an embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[0036] The present preferred embodiments of the invention are described herein with references to the drawings, wherein like components are identified with the same references. The descriptions of the preferred embodiments contained herein are intended to be exemplary in nature and are not intended to limit the scope of the invention.
[0037] FIG. 1 illustrates graphically an exemplary third generation, wireless, mobile access, Internet protocol (IP) data network 100 in which the invention will find application. For purposes of the present application, it is assumed the IP data network 100 adheres to the International Mobile Telecommunications 2000 (IMT-2000) standards and the specification of the International Telecommunications Union (ITU) for wireless, mobile access networks. Additionally, it is assumed that the data network 100 implements Mobile IP support according to the proposed Mobile IP version 4 (IPv4) standard of the Internet Engineering task Force (IETF). However, those skilled in the art will appreciate that the present invention can also be used in data networks that implement the Mobile IPv6 protocols. Thus, it should be noted that throughout this application, the term "agent" may be used interchangeably with the term "access router" or just "router" and so may "Agent Discovery" with "Neighbor Discovery," "Agent Solicitation" with "Router Solicitation" and "registration request" with "binding update." Especially, the term "agent" and the term "router" or "access router" may be collectively referred to as "mobility serving node" in this application. The Mobile IPv6 protocols are prescribed in the draft working document <draft-ietf-mobileip-ipv6-13> entitled "Mobility Support in IPv6," which is incorporated herein by reference.
[0038] The wireless, mobile access, IP data network 100 has at its core a fixed node IP data network 120 comprising numerous fixed nodes (not shown), i.e., fixed points of connection or links. Digital data is communicated within and over the network in accordance with Internet Protocol version 4 (IPv4), specified as IETF Requests for Comments (RFC) 2002, which is incorporated herein by reference. Again, IPv4 is just an example of communication protocol and can be replaced with other communication protocols, such as IPv6. Some of the nodes of the core network 120 comprise conventional routers (not shown), which function as intermediary nodes in accordance with conventional Internet addressing and routing protocols to route packets of data between source and destination nodes connected to the network.
[0039] Built on the core 120 is a collection of gateway routers (GR) 130 that comprise an IP mobile backbone 140. The gateways 130 comprising the IP mobile backbone are themselves nodes of the core network 120 and are interconnected via the core network 120. Each gateway 130 has a plurality of agents 145 connected thereto that can communicate with mobile nodes 135. Mobile nodes may comprise any number of different kinds of mobile, wireless communication devices including handsets, cellular telephones, hand-held computers, personal information managers or the like. The agents 145 are mobility serving nodes and function as home agents (HA) and foreign agents (FA) to interface mobile nodes 135 to the core network 120 through gateways 130, as specified in IETF RFC 2002. The agents 145 are Layer 3 access network entities. The mobile nodes 135 communicate with the agents 145 through radio access points (AP) 155. The APs 155 are Layer 2 access network entities. A group of APs 155 forms a subnetwork 150. Each agent 145 serves a subnetwork 150 and provides a network link as an interface between the subnetwork 150 and the data network 100. The mobile nodes 135 and the APs employ known CDMA or W-CDMA or similar digital data communication technology to communicate with each other.
[0040] Pursuant to RFC 2002, each mobile node is assigned a home radio subnetwork which comprises a home agent 145, which maintains current location information of the mobile node and which can route packets to the mobile node at its current location. Other agents 145 function as foreign agents, which a mobile node can "visit" while away from its home subnetwork area. Whichever home agent or foreign agent a mobile node 135 happens to be communicating with at a given time establishes a network link and provides network access to the mobile node. Each of the mobile nodes and agents in the network has a unique IP address just as in conventional fixed node data networks employing conventional Internet protocols.
[0041] Within the overall data network 100, two levels of handoff process are contemplated. The first level is a macro-level handoff or an Layer 3 handoff, which involves a change in location of a mobile node such that it leaves one radio subnetwork served by one agent to go to another subnetwork served by another agent. Thus, through an L3 handoff, the mobile node's network link necessarily changes. The next level is a micro-level handoff or an Layer 2 handoff, which involves a change in the location of a mobile node within an AP subnetwork 150, in which case the mobile node's radio link changes but network link does not change. The handling of L2 handoff is standard in wireless, cellular communication networks. For example, it is well known to use beacon signal strength from nearby APs for detecting reachability of the nearby APs.
[0042] FIG. 2 provides a simplified graphical illustration of the standard Mobile IP L3 handoff process. The network 120 is an IP data network that implements IPv4. Connected through gateways (not shown) to the network 120 are mobility agents 145 (HA, FA1, FA2 and FA3), each of which, as described above, operates its own subnet 150 that consists of a

group of APs 155 (not shown). Each subnet has a radio access network (RAN) or radio network controller (RNC) that keeps track of and maintains location information of all the MNs situated within its own subnet.
[0043] A MN 135 is currently located at a starting location A which is within the subnet operated by the FA1 and moving towards an end location C via an intermediary location B. The MN has originated from the HA and thus has a permanent home IP address given by the HA. But being within the FA1's subnet away from the HA's subnet, the MN has temporarily configured itself with a care-of address (CoA) provided by the FA1. Through the Mobile IP registration process that the MN previously performed with the FA1, the CoA has been registered in the HA as binding information. Therefore, any data that is destined to the MN is intercepted by the HA, tunneled to the FA1 and forwarded to the MN from the FA1. Outbound data from the MN may be routed back to the HA or sent directly to its destination.
[0044] As the MN moves from the starting location A and arrives at the intermediary location B, there comes a point where further wireless communication with the FA1 begins to fail. The MN is leaving the subnet 150 operated by the FA1 and about to enter the subnet 150 operated by the FA2. As the MN passes the intermediary location B, an L2 trigger is fired to inform the MN, FA1 and FA2 that the MN's L2 handoff is imminent. The trigger is fired sufficiently before the MN loses its radio link with the FA1 so that the MN can complete the L2 handoff to the FA2 before it loses the FA1. The L2 handoff is collaborative action by the MN, FA1 and FA2 and assisted by the RANs of FA1 and FA2. Upon completion of the L2 handoff, the MN has a new radio link with the subnet 150 operated by the FA2. Also, as soon as the MN enters the FA2's subnet, it begins to receive Agents Advertisements from the FA2. The Agents Advertisements from the FA2 inform the MN that it is now operating in the subnet served by the FA2.
[0045] As moving further towards the destination location C, the MN performs an L3 handoff or standard Mobile IP registration with the FA2. At the beginning of the registration process, the MN extracts a CoA from an Agent Advertisement from the FA2. Preferred procedures for address auto-configuration are specified in IETF RFC 2462, which is incorporated herein by reference. The MN's new CoA includes the FA2's IP address and a subnet address component for the MN as advertised by the FA2. The MN then registers the new CoA by sending, to the HA through the FA2, a registration request containing both the new CoA and the MN's permanent home IP address. In response, the HA updates the binding information of the MN in its binding cache and sends the MN a registration replay through the FA2, whereby an L3 link is established between MN and FA2. Hereafter, packets transmitted to the home IP address of the MN will be intercepted by the HA and tunneled by the HA to the FA2 and delivered to the MN from the FA2.
[0046] Please note that during the above standard Mobile IP registration process, there is a time period created during which the MN is unable to send or receive data. This time period is referred to as handoff latency, which starts at the time when the MN loses its radio communication with the FA1 and ends at the time when the MN completes the L3 handoff to the FA2. It has been calculated that the handoff latency introduced during the above registration process will probably fall in the range of more than hundreds of msecs. The contributing factors to this handoff latency appear to be the new agent discovery by the MN, the updating procedures at the HA, and probably most significantly, propagation of the registration request and replay messages between HA and FA2, which are likely to be separated by other intermediate local networks. The handoff latency resulting from the above standard Mobile IP registration process could be greater than what is acceptable to support real-time or delay sensitive traffic.
[0047] The present invention provides basically two schemes for minimizing latency associated with L3 handoffs. The first scheme is called a Pre-L2 handoff Mobile Initiated Tunneling handoff (Pre-MIT), and its detailed steps are illustrated in FIGS. 3a, 3b and 3c. The second scheme is called a Post-L2 handoff Mobile Initiated Tunneling (Post-MIT), and its detailed steps are illustrated in FIGS. 4a, 4b and 4c. Each scheme may operate under either trigger mode or trigger-less mode. With reference to FIGS. 3a, 3b and 3c, the Pre-MIT will first be described.
[0048] FIG. 3a is a graphical representation illustrating a Pre-MIT for IPv4. FIG. 3b is a diagram illustrating trigger mode timing analysis for a Pre-MIT shown in FIG. 3b. In FIG. 3a, there are two FAs shown each of which has, as described above, its own subnet 150 that consists of a group of APs 155 (not shown). A MN has been registered with an old FA (oFA or source) and is currently sending and receiving data through the oFA. The MN is now moving away from the oFA towards a new FA (nFA or target). It is assumed that the oFA and the nFA support different radio access technologies. This assumption will also underlie the other embodiments discussed in the present application. Yet, it should be appreciated that the present invention is also applicable to handoffs between FAs that support the same radio access technology.
[0049] When the MN arrives at a certain point between oFA and nFA where data communication with the oFA begins to fail, the MN receives an L2 trigger informing that an L2 handoff is imminent (Step 301). An L2 trigger is an abstraction of a notification from Layer 2 that a certain event has happened or is about to happen. There are three kinds of L2 triggers contemplated in the present invention. The first trigger is a trigger that notifies that an L2 handoff is imminent. This first trigger may be received by any of the MN, the oFA and the nFA. The second trigger is called a link-down trigger that notifies the MN and the oFA that they have lost an L2 communication link that existed between them. The last trigger is called a link-up trigger that notifies the MN and the nFA that a new L2 communication link has been established between them.
[0050] In the present invention, the L2 trigger is not associated with any specific L2 signals but rather is based on the kind of L2 information that is or could be available from a wide variety of radio link protocols. Thus, the trigger may be implemented in a variety of ways. For instance, the L2 driver may allow the IP stack to register a callback function that is called when the trigger fires. The operating system may allow a thread to call into a system call for the appropriate trigger or triggers. The trigger may consist of a protocol for transferring the trigger notification and parameter information at either L2 or L3 between the new AP and the old AP. Alternatively, the trigger information may be available within the operating system kernel to the IP stack from the driver as an out of band communication. Also, triggers may come from any of the oFA, the nFA and even the radio access networks (RAN) or radio network controllers (RNC) that serve the subnets operated by the oFA and the nFA if those entities are capable of firing such L2 triggers. The MN may self-trigger itself if it is capable of firing the triggers.
[0051] Triggered by the L2 trigger notifying that an L2 handoff is imminent, the MN sends a mobile handoff request (HReq(m)) to the oFA (Step 302). This HReq(m) is in a special message format that comprises an Internet Control Message Protocol (ICMP) Field, which contains four values, as shown in FIG. 5. The four values in the ICMP field are a type value, a code value, a checksum value and a reserved value. These values are in a bit format. The type value indicates that the message is a mobile handoff request (HReq(m)). The code value is 0. The checksum value is a 16-bit one's complement of the one's complement sum of the ICMP message, starting with the ICMP type value. For computing the checksum, the checksum field is set to 0. The reserved value is 32 bits that are set at 0.
[0052] The other field in the special message format is an Address field. The Address field contains target trigger parameters that are in a bit format. The target trigger parameters are link layer addresses or L2 identifiers (e.g., L2 addresses) of up to three target foreign agents. The MN may obtain these L2 identifiers from pilot beacon signals received from FAs. The oFA may optionally choose one of these L2 identifiers according to predetermined policies. In this embodiment, for better understanding of the processes in the invention, it is assumed that the Address field contains

one address, i.e., the address of the nFA. It is also assumed that the oFA knows the IP address of nFA. Without the IP address of nFA, the oFA could not communicate directly with the nFA. There are two ways for the oFA to obtain the IP address of nFA. One way is to obtain it from the MN. If Agent Advertisements from the nFA reach the MN, the MN may obtain the IP address of nFA from the Agent Advertisements and attach the address to an HReq(m). The other way is to require the oFA to have a table caching IP addresses of nearby FAs in relation to their L2 identifiers. If there is no IP address attached to the HReq(m), the oFA will extract an L2 identifier from one of the extensions of the HReq(m). With this L2 identifier, the oFA searches the table to find the corresponding IP address. Formation of the table and its search operation will be discussed later in detail in the Pre-MIT triggerless mode scheme shown in FIG. 3c. It is assumed in this embodiment that an HReq(m) from the MN has extensions that contain both L2 and L3 identifiers of nFA.

[0053] When receiving the HReq(m) from the MN, the oFA extracts the L3 identifier stored in one of the extensions attached to the HReq(m) and determines that the MN is going to switch its point of attachment from itself to the nFA. The oFA then sends a Source Agent Handoff Request (HReq(s)) to the nFA (Step 303). When receiving the HReq(s) from the oFA, the new FA opens the extensions attached to the request and learns that the MN is about to handoff from oFA to itself. In response, the nFA sends a Handoff Reply (HRply(t)) back to the oFA (Step 304), whereby a tunnel is established between oFA and nFA. The tunnel may be unidirectional and used only to forward data from nFA to oFA. Alternatively, the tunnel may be bidirectional and used to forward data back and forth between oFA and nFA. The Handoff Reply from the nFA is forwarded by the oFA to the MN (step 305).

[0054] The HReq(s) and the HRply(t) are in a special message bit format identical to each other. FIG. 6 shows the message format of the HReq(s) and the HRply(t). The format contains a type value, an H bit, a N bit, an R bit, a M bit, a G bit, a T bit, a B bit, a lifetime value, a home area address of the MN, a home address of the MN, among which relevant to the present inventions are as follows: The type value indicates that the message is a handoff request (HReq) or a handoff reply (HRply). The H bit is a source-triggered hand off request. When the H bit is set, then the N bit is unset that indicates that the request is from a source. The N bit is a target triggered handoff request. When set and the H bit is unset, this is an indication that the request is from a target. In this embodiment, the oFA is sending the HReq. Thus, H is set and N is unset. The R bit is set if the request is a request to renew a tunnel when neither the H nor the N bits are set. The T bit indicates that the oFA is willing to support both forward and reverse tunnel service. Thus, the oFA may decide according policies whether to make the tunnel unidirectional or bidirectional. The B bit indicates that the MN has requested a reverse tunnel to the HA and that the nFA should use reverse tunnel to the HA if it will not be reverse tunneling to the oFA.

[0055] Next, the lifetime value indicates the time in seconds for which tunnel service for the MN will be maintained. If the lifetime value is zero and the T bit is not set, then the oFA is not willing to tunnel any packets for the MN. A positive lifetime value and a set T bit indicate that the oFA is willing to tunnel for the indicated time. The identification value is a 64 bit number utilized for matching registration requests with registration replies, and for protecting against replay attacks of registration messages.

[0056] As long as the L2 link remains up between oFA and MN, the oFA forwards to the MN data tunneled from the MN's HA, and tunnels back to the HA or sends out directly to the destination data received from the MN. When the link with the MN becomes down, the oFA, notified by a link down trigger, will start sending data received for MN to the nFA through the tunnel established between oFA and nFA. As soon as the MN enters the subnet operated by the nFA and an L2 link is established between MN and nFA, the nFA, notified by a link up trigger, will deliver to the MN data tunneled from the oFA and may tunnel data from the MN back to the oFA if the tunnel is bidirectional.

[0057] Thus, the above embodiment of the present invention allows the MN to utilize L2 triggers to set up a tunnel between oFA and nFA that allows the MN to continue using the oFA for data communication while on the nFA's subnet. This eliminates a possible source of handoff latency and enables a rapid establishment of service at the new point of attachment while minimizing the impact on real-time applications. The MN must eventually perform a formal Mobile IP registration illustrated in FIG. 2 after L2 communication with a new FA is established, but this can be delayed as required by the MN. Until the MN performs registration, a new FA and an old FA will setup and move a tunnel as required to give MN continued connectivity.

[0058] FIG. 3c illustrates a timing analysis of the Pre-MIT method operating under the trigger-less mode. Under this trigger-less mode, it is assumed that the oFA has a table storing the IP addresses and L2 identifiers of nearby FAs. These addresses are obtained in advance, using Router Solicitations and Router Advertisements defined in Mobile IPv4 (RFC 2002). The difference between the present invention and RFC 2002 is that in RFC 2002, these protocols are implemented between an MN and nearby FAs, whereas the same protocols are implemented between a FA and its neighboring FAs in the present invention. Thus, in this embodiment, the old FA sends out Agent Solicitations in advance to neighboring FAs. In response, the neighboring FAs return Agent Advertisements to the oFA. The oFA then extracts the L3 identifiers and L2 identifiers from extensions attached to the Advertisements and cashes them in the internal table.

[0059] It is also assumed under the trigger-less mode that no L2 trigger is available for MN to initiate the Pre-MIT. Therefore, the MN has to use its internal L2 signals to initiate the Pre-MIT. If the MN's L2 has the link evaluation capability, when it sees link degradation, it can notify the MN's L3 for handoff. Usually, MN's L2 is designed to be able to monitor the signal strengths of pilot beacons from nearby FAs including the one with which the MN is communicating. By monitoring the beacon signal strengths, the L2 can notify the L3 that an L2 handoff is imminent. The L2 may also provide prioritized possible new candidate FAs and their L2 identifiers in the notice to the L3. Alternatively, the MN may use L3 evaluation of packet latency to predict an L2 handoff. Such handoff prediction based on packet latency is described in U.S. patent application Ser. No. 09/770,544 entitled "MOBILITY PREDICTION IN WIRELESS, MOBILE ACCESS DIGITAL NETWORKS" by Gwon et al. and U.S. patent application Ser. No. 09/772,381 entitled "FAST DYNAMIC ROUTE ESTABLISHMENT IN WIRELESS, MOBILE ACCESS DIGITAL NETWORKS USING MOBILITY PREDICTION" by Gwon et al., both of which are hereby incorporated by reference.

[0060] Returning to FIG. 3c, while connected to the oFA, the MN monitors pilot beacons from the oFA and other nearby FAs to find candidate FAs for next handoff. The MN is traveling away from the oFA towards a new FA. There comes a point between oFA and nFA where the MN receives a notice from its L2 that the pilot beacon from the oFA is fading. Using this notification from the L2 as a trigger, the MN initiates the Pre-MIT (Step 301). It is assumed that the L2 has already notified the MN, based on the signal strength of received pilot beacons, that the nFA is the target of next handoff. When initiating the Pre-MIT, the MN attaches the L2 identifier of nFA to an Agent Solicitation and sends it to the oFA (Step 302).

[0061] When receiving the Agent Solicitation from the MN, the oFA opens the extension and extracts the L2 identifier from it. The oFA then searches the table for the IP address corresponding to the received L2 identifier and determines the IP address of nFA. The oFA then sends a HReq(s) to the nFA (Step 303). This HReq(s), as well as a HRply(t) sent in next Step 304, has the same data format as shown in FIG. 6. The operations performed in Step 304 and Step 305 in FIG. 3c are the same as those performed in the corresponding steps in FIG. 3b and therefore a detailed description thereof is omitted. Under the trigger-less mode, the MN is able to initiate the Pre-MIT without any assistance from other

IP entities. Thus, the trigger-less mode is particularly suitable in situations where the hand-off is performed between FAs that support different radio access technologies. In some of the networks, e.g., IEEE 802.11x and Bluetooth, the L2 triggers as discussed above may not be available from the network side. According to the present invention, mobile nodes operating under the trigger-less mode can initiate the Pre-MIT between such heterogeneous networks irrespective of what radio access technologies these network supports.

[0062] FIG. 4a shows a Post-L2 handoff Mobile Initiated Tunneling Handoff (Post-MIT) scheme according to the present invention. FIG. 4b illustrates a timing analysis of the Post-MIT trigger mode scheme. FIG. 4c illustrates a timing analysis of the Post-MIT triggerless scheme. The difference between the Pre-MIT and the Post-MIT is that the Pre-MIT is initiated while the MN is within the oFA's subnet and has L2 connectivity to the oFA, whereas the Post-MIT is initiated after the MN enters the nFA's subnet (already lost L2 connectivity to the oFA) and establishes new L2 connectivity to the nFA. In other words, in the Pre-MIT, a tunnel between oFA and nFA is established while the MN is within the oFA's subnet before it begins an L2 handoff from the oFA to the nFA. In the Post-MIT, however, the tunnel is established after the MN enters the nFA"s subnet and the L2 handoff is completed to the nFA. Thus, the Pre-MIT may be characterized as "predictive" because a tunnel is established based on a predicted L2 handoff. The Post-MIT may be characterized as reactive because a tunnel is established subsequently to the establishment of new L2 connectivity to a new foreign agent.

[0063] The Post-MIT illustrated in FIG. 4b is initiated when the MN enters the subnet operated by the nFA. When leaving the oFA's subnet, the MN receives an L2 trigger informing that an L2 handoff is imminent, but the MN just ignores the trigger and let an L2 handoff take place. As soon as the MN enters the nFA's subnet, L2 connectivity is established between MN and nFA. The MN is notified of the fact by a link-up trigger (Step 401) and proceeds to initiate the Post-MIT. Alternatively, the MN may proceed with the standard Mobile IP registration process with the nFA. If the MN chooses to perform the standard registration process, the process will add to the handoff latency during which the MN will not be able to receive or send date until the registration process ends. If the MN was in the middle of sending or receiving delay sensitive data when the L3 connectivity to the oFA was lost, it should proceed with the Post-MIT according to the present invention.

[0064] Initiated by the link-up trigger, the MN sends the nFA a HReq(m) (Step 402) the data format of which is already shown in FIG. 5. The difference is that the HReq(m) used in the Pre-MIT method has an extension that contains the nFA's L2 identifier (L3 identifier is optional), whereas the HReq(m) used in the Post-MIT has an extension containing the oFA's IP address. When receiving the HReq(m), the nFA sends a HReq(t) to the oFA (Step 403). The oFA then returns a HRply(s) (Step 404). Through an exchange of the HReq(t) and the HRply(s) between nFA and oFA, a tunnel is established between them. The HRply(s) from the oFA is relayed to the MN from the nFA (Step 405) to notify the MN that a tunnel has been established. The HRply(s) from the oFA may be forwarded to the MN when the first data is sent to the MN through the tunnel. The HReq(t) and the HRply(s) are in the same message format as shown in FIG. 6. Since the HReq(t) is sent from the nFA (target) to the oFA (source), the H bit is unset and the N bit is set in the HReq(t). If the T bit is set in the HReq(t), the nFA is requesting reverse tunnel service. Also, a time indicated in the Lifetime represents a request by the nFA for a reverse tunnel. A value of 0 in the Lifetime indicates that the nFA does not require reverse tunnel service.

[0065] Using the tunnel between oFA and nFA, the MN, although being within the nFA's subnet, is able to receive data from the oFA. In the Post-MIT, the MN is not able to receive data until a tunnel is set up between nFA and oFA after it receives a link-up trigger. However, time for setting up the tunnel between nFA and oFA is considered minimal, compared to time required for the MN to perform the complete Mobile IP registration process in which registration request and reply messages propagate through intermediate networks between MN and its HA. Thus, like the Pre-MIT, the Post-MIT eliminates a possible source of handoff latency and enables a rapid establishment of service at the new point of attachment. The MN must eventually perform an L3 handoff somewhere, but this can be delayed as required by the MN.

[0066] FIG. 4c shows a time analysis of the Post-MIT operating under the triggerless mode. As in the Pre-MIT under the triggerless mode, no L2 trigger may be available for the MN to initiate the Post-MIT. Therefore, the MN must use its internal L2 signals to initiate the Post-MIT (Step 401). The MN's internal L2 signals that may be used for this purpose are internal link-up and link-down notifications generated from a protocol stack in the MN's link layer and brought up to the IP interface via an API by means of translating information available at the MN's device driver. Unlike the link-up or link-down trigger used in the trigger mode, these link-up and link-down notifications do not need to include any L2 or L3 identifier of the AP which the MN is connected to or disconnected from. For example, in wLAN IEEE 802.11b, the internal link-up and link-down notifications can be generated via a wLAN device driver when it receives a disassociation or re-association message created at the wLAN control frame.

[0067] Triggered by the internal L2 signal, the MN sends the nFA an Agent Solicitation with an extension containing the IP address of oFA (Step 402). The subsequent operations performed in Steps 403, 404 and 4055 are the same as the corresponding steps in FIG. 4b. This triggerless mode is particularly useful in situations where the Post-MIT is performed over heterogeneous networks that support different radio access technologies.

[0068] The present invention may also be used in networks that implement Mobile IPv6. FIGS. 7a and 7b are diagrams illustrating a Pre-L2 handoff Mobile Initiated Tunneling handoff (Pre-MIT) for Mobile IPv6 and its time analysis. There is no difference in basic protocols between the Pre-MIT for IPv6 and the counterpart for IPv4 already discussed above. The differences between them mainly reside in L3 messages used to implement the handoff operations. Like the Pre-MIT for IPv4, the Pre-MIT for IPv6 establishes a tunnel between an old access router (oAR) and a new access router (nAR) before an L2 handoff takes place from the oAR to the nAR. The tunnel so established will allow the MN to continue using the oAR for data communication while on the nAR's subnet. This eliminates a possible source of handoff latency and enables a rapid establishment of service at the new point of attachment while minimizing the impact on real-time applications.

[0069] Like the counterpart for IPv4, the Pre-MIT for IPv6 functions under either trigger or triggerless mode. Mobile IPv6 is designed to be more L2 independent than Mobile IPv4. But if the L2 trigger notifying that an L2 handoff is imminent is available in the IPv6 network, that L2 trigger may be used to trigger the MN to initiate the Pre-MIT according to this embodiment. If the L2 trigger is not available in the network, the Pre-MIT should be performed under the triggerless mode. Under the triggerless mode, if the MN has L2 capable of evaluating the link, the MN may use signaling from the L2 notifying link degradation. Alternatively, the MN may use L3 evaluation of packet latency to predict an L2 handoff.

[0070] As is required to implement the Pre-MIT for IPv4, the L2 identifier and/or L3 identifier of the nAR is also required to implement the Pre-MIT for IPv6. The MN can know the L2 identifier from beacon signals from the nAR. The MN can also know the L3 identifier from Router Advertisements from the nAR if the Router Advertisements reach the MN. The oAR may, on behalf of the MN, send Router Solicitations in advance to solicit Router Advertisements from the nearby ARs. When receiving Router Advertisements, the oAR cashes in a table the L3 identifiers of the nearby ARs in relation to their L2 identifiers. The table is used to identify the L3 identifier of the nAR when the MN notifies the oAR of only the L2 identifier of the nAR.

[0071] Returning to FIGS. 7a and 7b, triggered by either external or internal signaling that an L2 handoff is imminent

(Step 701), the MN prepares a Mobile Handoff Initiation Message HI(m) and sends the HI(m) to the oAR (Step 702). This HI(m) is in a special message format that comprises an IP Field, an Internet Control Message Protocol (ICMP) Field and Option Field. The ICMP Field is shown in FIG. 9. The IP Field contains four values which provide parameters necessary to deliver a Handoff Initiation Message (HI) from a sender to a receiver. The first value in the IP Field is a Source Address, which is the MN's home IP address in this embodiment. The second value is a Destination Address, which is the oAR's IP address in this embodiment. The third value is a Hop Limit which is set to 255. The last value is an Authentication Header as required by IPv6 security protocol. This Authentication Header will be used to authenticate the HI to the receiver.

[0072] In the ICMP Field, the type value indicates that the message is a mobile handoff initiation message (HI(m)). The code value is 0. The checksum value is a 16-bit one's complement of the one's complement sum of the ICMP message, starting with the ICMP type value. The Identifier value indicates the sender of the message, which is the MN in this embodiment. The S bit is set to 0. The U bit is a buffer flag. When the U bit is set, until the MN becomes ready to receive data in the nAR'subnet, the nAR is required to buffer any packets destined for the MN that are tunneled from the oAR. The H bit is a Pre-MIT flag which indicates, when set, that the handoff operation is the Pre-MIT. The T bit is a Post-MIT flag, which indicates, when set, that the handoff operation is the Post-MIT. The R bit is set at 0. The M bit is a mobile initiation flag which indicates, when set, that the MN is initiating the MIT handoff. The Reserved value is set to 0.

[0073] There are five valid values that may be stored in the Option Field. The first value is the link layer (L2) address of the MN. This value should be included in the Field to help the destination recognize the MN. The second value is the link layer address of the nAR. The third value is the IP (L3) address of the nAR. In order to perform the Pre-MIT, either the link layer address or the IP address of the nAR has to be included in the Field to notify the oAR of the identity of the nAR, to which the MN is expecting to handoff. The forth value is the IP address of the oAR, which will be presented from the MN to the nAR when initiating the Post-MIT as discussed later. The last value is a new care of address (CoA) of MN. The MN's CoA includes nAR's IP address and a subnet address component for the MN as advertised by the nAR.

[0074] In FIGS. 7a and 7b, the HI(m) is sent to the nAR (Step 702). If the L3 identifier of the nAR is not included in the HI(m), the oAR searches the table for the L3 identifier corresponding to the L2 identifier of the nAR stored in the HI(m). The oAR then prepares a Source Handoff Initiation Message (HI(s)) and sends the HI(s) to the nAR (Step 703). The HI(s) is in a format that comprises an IP Field, ICMP Field and Option Field. The ICMP Field is illustrated in FIG. 10. In the IP Field, the Source Address is now the IP address of the oAR in this embodiment because the oAR is sending the HI(s). The Destination Address is set to the IP address of the nAR. The values in the ICMP Field are transported from the HI(m) sent from the MN. The Option Field includes: the link-layer address of the MN; the old CoA used by the MN while attached to the oAR; a new CoA that the MN wants to use when connected to the nAR; and a lifetime of a tunnel, in seconds, for which the oAR requests the tunnel to be maintained.

[0075] In response, the nAR returns a Handoff Acknowledgement Message (HACK) to the oAR (Step 704), whereby a bidirectional or unidirectional tunnel is established between oAR and nAR. The HACK is in a data format that comprises an IP Field, ICMP Field and an Option Field. The ICMP Field is shown in FIG. 11. In the IP Field, the Source Address is the IP address of the nAR. The Destination Address is set to the IP address of the oAR. In the ICMP Field, the code value may be set at one of "128," "129" and "130" when the nAR cannot accept the handoff. The value "128" means to the receiver, i.e., the oAR, that the sender, i.e., the nAR, cannot accept the handoff for unspecified reasons. The value "129" means that the sender cannot accept the handoff because it is administratively prohibited. The value "130" means that the sender cannot accept the handoff because of insufficient resources. The Option Field includes a lifetime of a tunnel, in seconds, for which the sender, i.e., the nAR in this embodiment, is willing to grant tunnel service.

[0076] The HACK from the nAR is forwarded from the oAR to the MN (Step 705). If the MN finds any one of the above three values in the ICMP Field, the MN will perform the standard Mobile IPv6 registration process by sending out a Router Solicitation to find out candidate new access routers for handoff. If the MN fails to receive the HACK from the oAR within a certain period of time after it sent the HI(m) to the oAR, the MN will likewise proceed to perform the standard Mobile IPv6 registration process.

[0077] FIGS. 8a and 8b are diagrams illustrating a post-mobile initiated tunneling (Post-MIT) handoff for Mobile IPv6 and its time analysis. There is no difference in basic protocols between the Post-MIT for IPv6 and the counterpart for IPv4 already discussed above. The differences between them mainly reside in L3 messages used to implement the handoff operations. Like the counterpart for IPv4, the Post-MIT for IPv6 establishes a tunnel between an old access router (oAR) and a new access router (nAR) after new L2 connectivity is established between MN and nAR. The Post-MIT eliminates a possible source of handoff latency and enables a rapid establishment of service at the new point of attachment.

[0078] The Post-MIT illustrated in FIGS. 8a and 8b is initiated by the MN, as receiving a link-up trigger when the MN enters the subnet of nFA (Step 801). Initiated by the link-up trigger, the MN prepares a Mobile Handoff Initiation Message HI(m) and sends it to the nAR (Step 802). In the HI(m), the IP Field has the IP address of the nAR as the Destination Address. In the ICMP Field, the H bit is unset and the T bit is set. Instead of the link layer and/or IP address of the nAR, the Option Filed has the IP address of the oAR. Upon receipt of the HI(m) from the MN, the nAR prepares a Target Handoff Initiation Message (HI(t)) and sends it to the oAR (Step 803). The oAR returns a HACK to the nAR (Step 804), whereby a bi-directional or unidirectional tunnel is established between oAR and nAR. In the HI(t), the IP Field has the IP address of the nAR as the Source Address in this embodiment. The Destination Address is set to the IP address of the oAR. The values in the ICMP Field are transported from the HI(m) sent from the MN. The Option Field includes a lifetime of a tunnel, in seconds, for which the nAR requests the tunnel to be maintained.

[0079] In the HACK from the oAR, the IP Field has the IP address of the oAR as the Source Address in this embodiment. The Destination Address is set to the IP address of the nAR. In the ICMP Field, the code value may be set at one of "128," "129" and "130" when the nAR cannot accept the handoff. These values have the same meanings as described above. The Option Field includes a lifetime of a tunnel, in seconds, for which the sender in this embodiment, i.e., the oAR, is willing to grant tunnel service.

[0080] The HACK from the nAR is forwarded from the oAR to the MN (Step 805). If the MN finds any one of the three values in the code, the MN will perform the standard Mobile IPv6 registration process with the nAR. Likewise, if the MN fails to receive the HACK from the oAR within a certain period of time after it sends the HI(m) to the nAR, the MN will proceeds to perform the standard Mobile IPv6 registration process.

[0081] It should be appreciated that the foregoing detailed description is illustrative rather than limiting, and that it is the following claims, including all equivalents, that are intended to define the spirit and scope of this invention. For instance, although only MN is the initiator of the Pre and Post MIT handoffs in the above embodiments, other IP entities, such as oFA (oAR), nFA (nAR) and even a radio access network located in the subnet operated by the oFA (oAR) or the subnet operated by the nFA (nAR), may initiate the handoffs of the present invention.

LOW LATENCY MOBILE INITIATED TUNNELING HANDOFF

Claims of correspondent: **US 2003104814 (A1)**

1. A method of implementing a low latency handoff by a mobile node between source and target nodes that support different radio access technologies, comprising the steps of:
triggering at least one of the mobile node, the source node and the target node to initiate the handoff process;
establishing, upon initiated, a tunnel between the source and target nodes; and
using the tunnel for data communication between the mobile node and the source node after the mobile node completes an L2 handoff from the source node to the target node but before undergoing IP routing update with the target node.

2. A method according to claim 1, wherein the mobile node is triggered to initiate the handoff process.

3. A method according to claim 2, wherein the mobile node, upon triggered, sends a tunneling handoff request to the source node.

4. A method according to claim 3, wherein the mobile node obtains an L2 identifier of the target node and includes the L2 identifier in the tunneling handoff request.

5. A method according to claim 4, wherein the source node creates a table containing L3 identifiers of neighboring networks in relation to their L2 identifiers and looks up the table for an L3 identifier that corresponds to the L2 identifier in the tunneling handoff request from the mobile node.

6. A method according to claim 3, wherein the mobile node obtains an L3 identifier of the target node and includes the L3 identifier in the tunneling handoff request.

7. A method according to claim 1, wherein the tunnel is established before the mobile node completes the L2 handoff between the source and target nodes.

8. A method according to claim 1, wherein the tunnel is established after the mobile node completes the L2 handoff between the source and target nodes.

9. A method according to claim 1, wherein the trigger is generated externally of the mobile node.

10. A method according to claim 1, wherein the trigger is generated internally of the mobile node.

11. A method according to claim 1, wherein the mobile node utilizes L2 signaling to initiate the handoff process.

12. A method according to claim 1, wherein the mobile node utilizes L2 signaling to initiate the handoff process.

13. A method according to claim 2, wherein the mobile node, upon triggered, sends a tunneling handoff request to the target node.

14. A method of implementing a low latency handoff by a mobile node between source and target nodes, comprising the steps of:
triggering the mobile node to initiate the handoff process;
establishing, upon initiated, a tunnel between the source and target nodes; and
using the tunnel for communication between the mobile node and source node after the mobile node completes an L2 handoff from the source node to the target node but before undergoing IP routing update with the target node.

15. A method according to claim 14, wherein the mobile node, upon triggered, sends a tunneling handoff request to the source node.

16. A method according to claim 15, wherein the mobile node obtains an L2 identifier of the target node and includes the L2 identifier in the tunneling handoff request.

17. A method according to claim 16, wherein the source node creates a table containing L3 identifiers of neighboring nodes in relation to their L2 identifiers and looks up the table for an L3 identifier that corresponds to the L2 identifier in the tunneling handoff request from the mobile node.

18. A method according to claim 15, wherein the mobile node obtains an L3 identifier of the target node and includes the L3 identifier in the tunneling handoff request.

19. A method according to claim 14, wherein the tunnel is established before the mobile node completes the L2 handoff from the source node to the target node.

20. A method according to claim 14, wherein the tunnel is established after the mobile node completes the L2 handoff from the source node to the target node.

21. A method according to claim 14, wherein the trigger is generated externally of the mobile node.

22. A method according to claim 14, wherein the trigger is generated internally of the mobile node.

23. A method according to claim 14, wherein the mobile node utilizes L2 signaling to initiate the handoff process.

24. A method according to claim 14, wherein the mobile node utilizes L3 signaling to initiate the handoff process.

25. A method according to claim 14, wherein the mobile node, upon triggered, sends a tunneling handoff request to the target node.

26. A mobile node that performs a low latency handoff between source and target nodes, comprising:
a controller that initiates the handoff upon triggered; and
a transmitter that sends, when the handoff is initiated, a tunneling handoff request to either the source or target node to establish a tunnel between the source and target nodes, wherein the tunnel is used for communication between the mobile node and the source node after the mobile node completes an L2 handoff from the source node to the target node but before undergoing IP routing update with the target node.

27. A mobile node according to claim 26, wherein the transmitter sends a tunneling handoff request to the source node.

28. A mobile node according to claim 27, wherein the mobile node comprises a receiver that obtains an L2 identifier of the target node, which will be included in the tunneling handoff request, wherein the source node has a table containing L3 identifiers of nearby nodes in relation to their L2 identifiers and looks up the table for a L3 identifier that corresponds to the L2 identifier in the tunneling handoff request from the mobile node.

29. A mobile node according to claim 27, wherein the mobile node comprises a receiver that obtains an L3 identifier of the target node, which will be included in the tunneling handoff request.

30. A mobile node according to claim 26, wherein the transmitter sends the tunneling handoff request before the mobile node completes an L2 handoff from the source node to the target node.

31. A mobile node according to claim 26, wherein the transmitter sends the tunneling handoff request after the mobile node completes an L2 handoff from the source node to the target node.

32. A mobile node according to claim 26, wherein the trigger is generated externally of the mobile node.

33. A mobile node according to claim 26, wherein the trigger is generated internally of the mobile node.

34. A mobile node according to claim 26, wherein the mobile node utilizes L2 signaling to initiate the handoff process.

35. A mobile node according to claim 26, wherein the mobile node utilizes L3 signaling to initiate the handoff process.

36. A mobile node according to claim 26, wherein the transmitter sends the tunneling handoff request to the target node.

---

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号
特開2003－209872
（P2003－209872A）
(43)公開日　平成15年７月25日(2003.7.25)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｑ　7/22		Ｈ０４Ｌ　12/56	１００Ｄ	５Ｋ０３０
Ｈ０４Ｌ　12/56	１００	Ｈ０４Ｂ　7/26	１０７	５Ｋ０６７
Ｈ０４Ｑ　7/28		Ｈ０４Ｑ　7/04	Ｋ	

審査請求　有　　請求項の数25　ＯＬ　（全 17 頁）

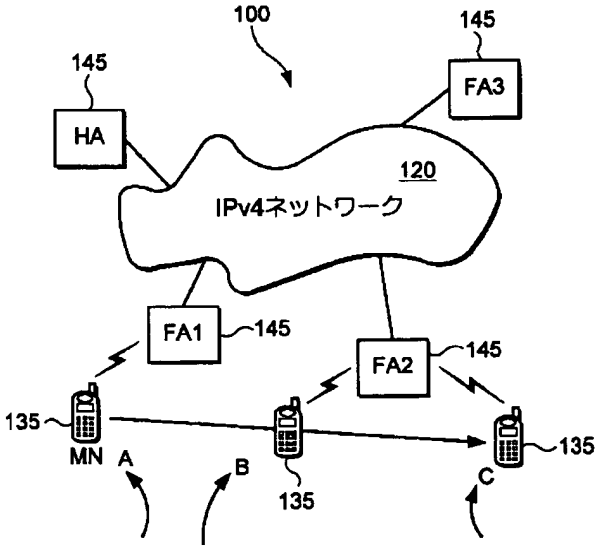
(21)出願番号　特願2002－348438(P2002－348438)
(22)出願日　平成14年11月29日(2002.11.29)
(31)優先権主張番号　６０／３３４４８１
(32)優先日　平成13年11月30日(2001.11.30)
(33)優先権主張国　米国（ＵＳ）
(31)優先権主張番号　１０／１３８３８９
(32)優先日　平成14年５月３日(2002.5.3)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　301077091
ドコモ　コミュニケーションズ　ラボラトリーズ　ユー・エス・エー　インコーポレーティッド
アメリカ合衆国，カリフォルニア州　95110，サンノゼ，スイート300，メトロドライブ　181
(74)代理人　100098084
弁理士　川▲崎▼　研二　（外１名）

最終頁に続く

(54)【発明の名称】　遅延の少ない移動機起動トンネリングハンドオフ

(57)【要約】
【課題】　ハンドオフ遅延を小さくする。
【解決手段】　本発明によれば、２つのモビリティサービス提供ノード（ソースノードとターゲットノード）との間にトンネルが確立される。トンネルは、モバイルノードがＬ２ハンドオフをソースノードからターゲットノードに行った後でかつ、ターゲットノードに関する標準モバイルＩＰ登録プロセス（すなわちＩＰルーティング更新）を行う前に、モバイルノードとソースノードとの間の通信に使用される。トンネルは、モバイルノードがＬ２ハンドオフをソースノードからターゲットノードに行う前もしくは後に確立されても良い。また、トンネルは、モバイルノードの内部もしくは外部で生成されたトリガによって確立されるのでも良い。



【特許請求の範囲】
【請求項１】　異なる無線アクセス技術を使用しているソースノードとターゲットノードとの間をモバイルノードが少ない遅延でハンドオフを実施する方法において、
ハンドオフプロセスを開始するために、モバイルノード、ソースノードおよびターゲットノードのうち最低１つをトリガする過程と、
ハンドオフプロセスが開始させられたら、ソースノードとターゲットノードとの間にトンネルを確立する過程と、
モバイルノードがレイヤ２ハンドオフを前記ソースノードから前記ターゲットノードに行った後でかつ、前記ターゲットノードに関するＩＰルーティング更新を行う前に、トンネルを使用して、前記モバイルノードと前記ソースノードとの間でデータ通信を行う過程とを有することを特徴とする方法。
【請求項２】　請求項２に記載の方法において、
前記モバイルノードはハンドオフプロセスを開始するためにトリガされることを特徴とする方法。
【請求項３】　ソースノードとターゲットノードとの間をモバイルノードが少ない遅延でハンドオフを実施する方法において、
ハンドオフプロセスを開始するためにモバイルノードをトリガする過程と、
ハンドオフプロセスが開始させられたら、ソースノードとターゲットノードとの間にトンネルを確立する過程と、
前記モバイルノードがレイヤ２ハンドオフを前記ソースノードから前記ターゲットノードに行った後でかつ、前記ターゲットノードに関するＩＰルーティング更新を行う前に、トンネルを使用して、前記モバイルノードと前記ソースノードとの間でデータ通信を行う過程とことを特徴とする方法。
【請求項４】　請求項２または３に記載の方法において、
前記モバイルノードは、トリガされたら、前記ソースノードにトンネリングハンドオフ要求を送信することを特徴とする方法。
【請求項５】　請求項４に記載の方法において、
前記モバイルノードは、前記ターゲットノードのレイヤ２識別子を取得して、これを前記トンネリングハンドオフ要求に含めることを特徴とする方法。
【請求項６】　請求項５に記載の方法において、
前記ソースノードは、近隣ノードのレイヤ３識別子とレイヤ２識別子とを関連付けたテーブルを作成し、前記モバイルノードからの前記トンネリングハンドオフ要求内に含まれる前記レイヤ２識別子に対応するレイヤ３識別子をこのテーブルから探すことを特徴とする方法。
【請求項７】　請求項４に記載の方法において、
前記モバイルノードは、前記ターゲットノードのレイヤ３識別子を取得して、そのレイヤ３識別子を前記トンネリングハンドオフ要求に含めることを特徴とする方法。
【請求項８】　請求項１または３に記載の方法において、
前記モバイルノードが前記ソースノードと前記ターゲットノードとの間のレイヤ２ハンドオフを完了する前に、前記トンネルは確立されることを特徴とする方法。
【請求項９】　請求項１または３に記載の方法において、
前記モバイルノードが前記ソースノードと前記ターゲットノードとの間のレイヤ２ハンドオフを完了した後に、前記トンネルは確立されることを特徴とする方法。
【請求項１０】　請求項１または３に記載の方法において、
前記トリガは、前記モバイルノードの外部で生成されることを特徴とする方法。
【請求項１１】　請求項１または３に記載の方法において、
前記トリガは、前記モバイルノード内部で生成されることを特徴とする方法。
【請求項１２】　請求項１または３に記載の方法において、
前記モバイルノードはハンドオフプロセスを開始するためにレイヤ２信号を利用することを特徴とする方法。
【請求項１３】　請求項１または３に記載の方法において、
前記モバイルノードはハンドオフプロセスを開始するためにレイヤ３信号を利用することを特徴とする方法。
【請求項１４】　請求項２または３に記載の方法において、
前記モバイルノードは、トリガされると、前記ターゲットノードにトンネリングハンドオフ要求を送信することを特徴とする方法。
【請求項１５】　ソースノードとターゲットノードとの間を少ない遅延でハンドオフを行うモバイルノードにおいて、
トリガされたら、ハンドオフを開始するコントローラと、
ハンドオフが開始したら、ソースノードとターゲットノードとの間にトンネルを確立するために、トンネリングハンドオフ要求を前記ソースノードか前記ターゲットノードかに送信する送信機とを有しモバイルノードがレイヤ２ハンドオフを前記ソースノードから前記ターゲットノードに行った後でかつ、前記ターゲットノードに関するＩＰルーティング更新を行う前に、前記トンネルを使用して、前記モバイルノードと前記ソースノードとの間でデータ通信を行うことを特徴とするモバイルノード。
【請求項１６】　請求項１５に記載のモバイルノードにおいて、
前記送信機は、前記ソースノードにトンネリングハンド

オフ要求を送信することを特徴とするモバイルノード。
【請求項１７】　請求項１６に記載のモバイルノードにおいて、
前記モバイルノードは、前記ターゲットノードのレイヤ２識別子を取得する受信機を有していて、
そのレイヤ３識別子は前記トンネリングハンドオフ要求に含められ、
前記ソースノードは、近隣ノードのレイヤ３識別子とレイヤ２識別子とを関連付けたテーブルを有し、前記モバイルノードからの前記トンネリングハンドオフ要求内に含まれる前記レイヤ２識別子に対応するレイヤ３識別子をこのテーブルから探すことを特徴とするモバイルノード。
【請求項１８】　請求項１６に記載のモバイルノードにおいて、
前記モバイルノードは、前記ターゲットノードのレイヤ３識別子を取得するための受信機を有していて、このレイヤ３識別子は前記トンネリングハンドオフ要求に含められることを特徴とするモバイルノード。
【請求項１９】　請求項１５に記載のモバイルノードにおいて、
前記モバイルノードが前記ソースノードと前記ターゲットノードとの間のレイヤ２ハンドオフを完了する前に、前記送信機はトンネリングハンドオフ要求を送信することを特徴とするモバイルノード。
【請求項２０】　請求項１５に記載のモバイルノードにおいて、
前記モバイルノードが前記ソースノードと前記ターゲットノードとの間のレイヤ２ハンドオフを完了した後に、前記送信機はトンネリングハンドオフ要求を送信することを特徴とするモバイルノード。
【請求項２１】　請求項１５に記載のモバイルノードにおいて、
前記トリガは、前記モバイルノードの外部で生成されることを特徴とするモバイルノード。
【請求項２２】　請求項２６に記載のモバイルノードにおいて、
前記トリガは、前記モバイルノード内部で生成されることを特徴とするモバイルノード。
【請求項２３】　請求項１５に記載のモバイルノードにおいて、
前記モバイルノードはハンドオフプロセスを開始するためにレイヤ２信号を利用することを特徴とするモバイルノード。
【請求項２４】　請求項１５に記載のモバイルノードにおいて、
前記モバイルノードはハンドオフプロセスを開始するためにレイヤ３信号を利用することを特徴とするモバイルノード。
【請求項２５】　請求項１５に記載のモバイルノードにおいて、
前記送信機は、前記ターゲットノードにトンネリングハンドオフ要求を送信することを特徴とするモバイルノード。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、デジタルデータネットワークにおけるデジタルデータ通信に関し、特に、インターネットプロトコルを基にした無線移動体アクセスデータネットワークにおけるデジタルデータ通信に関する。本発明は、特に、ボイスオーバーＩＰ（ＶｏＩＰ）やリアルタイムマルチメディアのようなリアルタイムインタラクティブデジタルデータ通信に関する。
【０００２】
【従来の技術】デジタル通信とパーソナル通信システムの発達と共に、パーソナル無線通信の必要性が高まっている。過去数年のセル式無線技術の発展とセル式電話システムの成長率は、無線による位置に依存しないセル式電話システムに対する高い需要が市場であると言うことを示している。無線つまり移動体セル式通信システムは、約２０年前に商用化された第１世代（１Ｇ）無線通信システムから世代ごとに変化しながら進化している。第１世代システムは、完全にアナログであり、主に音声通信のために使用された。現在、第３世代（３Ｇ）無線通信システムが導入されつつある。３Ｇは、ＩＭＴ－２０００グローバルフレームワークに基づいて、ＩＴＵによって規定されていて、Ｗ－ＣＤＭＡやＣＤＭＡ２０００のような新たな通信技術を使用する。３Ｇは、高速マルチメディアデータ・音声向けに設計されていて、その目的として、高品質音声・映像通信の達成そして世界中をローミングすることができることがある。つまり、どこにでも行けて、自動的に利用可能な無線システム（屋内電話システム、セル式、衛星式など）にハンドオフが行われると言うことである。前世代無線通信システムと違い、３Ｇシステムは、（システム構成によって違いはあるが）ＩＰを基にしている。つまり、データは全て発信元から宛先まで、インターネットで標準に使われるアドレス設定と経路付けのプロトコルによってデジタル形式で送られる。
【０００３】ＯＳＩ（Ｏｐｅｎ　Ｓｙｓｔｅｍ　Ｉｎｔｅｒｃｏｎｎｅｃｔｉｏｎ）モデルとして知られるものの多くの機能が、無線ＩＰ通信にも存在する。ＯＳＩ参照モデルでは７層の通信プロトコルを規定している。例えば、ＯＳＩモデルでは、階層プロトコルを規定していて、それは以下の様なものである。すなわち、低レベル物理ハードウェア仕様と接続（レイヤ１）、無線データリンク確立とフォーマット（レイヤ２）、ＩＰネットワークアドレス設定とルーティング（レイヤ３）、トランスポートルール（レイヤ４）、セッション（レイヤ５）、プレゼンテーション（レイヤ６）、アプリケーシ

ョン（レイヤ7）である。レイヤ2はノード間の無線リンクに関していて、特定の無線アクセス技術を実装している。レイヤ3（ＩＰ層と呼ばれることが多い）は、パケットすなわちＩＰデータのルーティングを行う。

【０００４】無線通信システムの発展の歴史の中に、無線通信の実現に関連した技術的問題が常にあった。それは、移動機（モバイルノード：ＭＮ）が、あるエリアから他のエリアに移動し、無線通信を行う無線アクセスポイント（ＡＰ）を不定期に変更することによる問題である。実際、優秀な移動体通信プロトコルとなるかどうかが決まるのは、ハンドオフの設計いかんによっている。このハンドオフは、ＭＮがある無線ＡＰから他の無線ＡＰに移動する時に発生するものである。無線ＡＰを単に変更するだけの場合は、「レイヤ２（Ｌ２）ハンドオフ」と呼ばれ、ＩＰ層のレイヤ３での信号のやりとりはなされない。もし新しい無線アクセスポイントが新しいサブネットに属していたら、つまりＭＮがあるサブネットから他のサブネットに移動したら、経路が変更され、レイヤ３（Ｌ３）でのプロトコル処理が必要になる。このＬ３でのプロトコル処理は、「Ｌ３ハンドオフ」と呼ばれ、普通このプロトコル処理ではＩＰメッセージの交換を行い、ＭＮの経路情報を更新して、ＭＮ宛のデータが新たなサブネットを経由してＭＮに確実に届くようにしている。

【０００５】インターネット技術標準化委員会（ＩＥＴＦ：The Internet Enginnering Task Force）は、ハンドオフ処理を扱ったいくつかの基準を提案している。例えば、モバイルＩＰバージョン４（ＩＰｖ４）と呼ばれているＩＥＴＦによるＲＦＣ２００２「ＩＰモビリティサポート」には、ＭＮが異なるエージェントによる異なったサブネット間でＬ３ハンドオフをどの様に行うかが記載されている。モバイルＩＰｖ４においては、ＭＮは、ホームエージェント（ＨＡ）からホームアドレスをもらい、ＭＮ自身が送信するＩＰデータ全てのソースアドレスとして使用する。ＭＮがホームサブネットから離れたフォーリンサブネット内に位置しているとき、ＭＮには、現時点での接続点を表している気付アドレス（ＣｏＡ）が対応付けられている。Ｌ３ハンドオフを通して、気付アドレスがＭＮのホームエージェントに登録されて、ＭＮに関するバインディング情報、すなわちデータ経路情報の更新がＨＡにより行われる。

【０００６】ＲＦＣ２００２によるＬ３ハンドオフプロセスでは、モビリティエージェント、すなわちフォーリンエージェントとホームエージェントとが必要であり、それぞれは、自身の存在をエージェント広告メッセージを通して知らせていなければならない。このエージェント広告を受信したＭＮは、自身はホームサブネット上で稼動しているのか、フォーリンサブネット上で稼動しているのかを判断する。ＭＮは自身が新しいサブネットに入ったと判定したら、ＭＮはそのフォーリンサブネットワークにサービスを提供しているフォーリンエージェントが送信しているエージェント広告から気付アドレスを取得する。ＭＮは、この気付アドレスを含んだ登録要求を自身のホームエージェントＨＡに送信して、新しい気付アドレスを登録する。ＨＡが登録要求を受信して、内部のＭＮに関するバインディング情報を更新して、ＭＮに登録返答を返すと、Ｌ３ハンドオフが終了する。登録が終了すると、ＭＮのホームアドレスに送られたデータは、ＨＡが受け取り、ＨＡがＭＮの気付アドレスにトンネル伝送する。トンネル伝送されたデータをトンネルの終点（ＦＡかＭＮ自身）が受信して、ＭＮに最終的に配送される。反対方向では、ＭＮが送信したデータは、ＩＰの経路付けメカニズムの標準に従って、ＨＡを経由する必要なしに宛先まで配送される。

【０００７】モバイルＩＰは、自身の下のリンク層に関して何も決めずに設計されている。それゆえ、モバイルＩＰは非常に適用可能な範囲が広い。このことにより、プロトコルスタックにおけるＬ２とＬ３との間を明白に分離すると言う有利な点が得られるが、不利な点もある。Ｌ２とＬ３が厳格に分離されているので、ＭＮは直接つながっているＦＡとしか通信できない。つまり、ＭＮは前のＦＡへのＬ２での接続を失った後、ＭＮは、新たなＦＡへのＬ２接続を得るまで、登録プロセスを開始することができない。さらに、登録要求と返答メッセージとがＭＮとＨＡ間のネットワークを伝送するのに時間がかかるために、登録プロセスに時間がかかる。ＭＮと旧ＦＡとの間のＬ３接続の終わりから、新ＦＡとの新たなＬ３接続までの時間が、ハンドオフ遅延である。この間、ＭＮはデータの送受信ができない。標準モバイルＩＰハンドオフ手順によるハンドオフ遅延は、リアルタイム通信や、遅延に敏感な通信には許容できない。

【０００８】ハンドオフ遅延量を削減するための様々なプロトコルが、モバイルＩＰｖ４とＩＰｖ６用に提案されている。例えば、インターネットドラフト「モバイルＩＰｖ４における遅延の少ないハンドオフ：ｄｒａｆｔ－ｉｅｔｆ－ｍｏｂｉｌｅｉｐ－ｌｏｗｌａｔｅｎｃｙ－ｈａｎｄｏｆｆｓ－ｖ４－０３．ｔｘｔ」は、モバイルＩＰ登録プロセスにおける遅延によって、ＭＮがデータの送受信ができない期間を削減するための技術を２つ提案している。１つは「前登録ハンドオフ」であり、ＭＮは旧ＦＡと接続しながら、新ＦＡと通信をすることができる。もう１つは「後登録ハンドオフ」であり、正式な登録プロセスが完了する前に、新ＦＡからのＭＮへのデータ配送が行われる。さらに詳しく説明すると、前登録ハンドオフにおいては、旧ＦＡは、Ｌ２トリガによって起動させられて、ＭＮに新ＦＡに関する通知を行う。すると、ＭＮは、旧ＦＡと通信を行いながら、すなわち旧ＦＡ経由でデータの送受信を行いながら、新ＦＡへのＬ３ハンドオフを開始する。すなわち、前登録ハンドオ

フでは、Ｌ２ハンドオフが始まる前にＬ３ハンドオフが始まってよく、これは新旧ＦＡの間で瞬断のないハンドオフを達成することに役立つ。新ＦＡは、旧ＦＡ経由でＭＮに存在を示して、前登録ハンドオフを開始してもよい。またＭＮは、旧ＦＡにプロキシルータ請求（ソリシテーション）を送って、前登録ハンドオフの起動者（イニシエータ）になっても良い。この時旧ＦＡは、このプロキシルータ請求に答えてＭＮに新ＦＡに関して通知する。いずれにせよ、前登録ハンドオフを実施するには、素早くタイミングよいＬ２トリガが必要である。

【０００９】後登録ハンドオフでは、旧ＦＡと新ＦＡとがＬ２トリガを使って、新旧ＦＡ間に双方向トンネル（ＢＤＴ）を作成し、これにより、ＭＮは新ＦＡのサブネット上にいるときでも、旧ＦＡを使用し続けることができるようになる。後登録ハンドオフもまた、新旧ＦＡのどちらかに与えられるＬ２トリガによって起動させられる。ＭＮと旧ＦＡとの間でのモバイルＩＰ登録が成功した後、旧ＦＡがＭＮにとってモビリティアンカーポイントになる。それから、旧ＦＡか新ＦＡのどちらかが、ＭＮが旧ＦＡから新ＦＡへと移動しそうであるとのＬ２トリガ情報を受信する。トリガを受信したＦＡ（旧ＦＡか新ＦＡ）は、他方のＦＡ（新ＦＡか旧ＦＡ）にハンドオフ要求を送信する。これを受信した他方のＦＡはハンドオフ返答を返す。これによって、ＦＡ間に双方向トンネルができる。旧ＦＡとＭＮとの間のリンクが切断されたら、旧ＦＡは、ＭＮ宛のデータをこのトンネルを介してＭＮに送り始める。新ＦＡとＭＮとの間にリンクが確立されたら、新ＦＡは、旧ＦＡからトンネルを通して送られてきたデータをＭＮに送り始め、またＭＮからのデータを旧ＦＡに逆方向に転送する。Ｌ２ハンドオフが完了したら、ＭＮは、データを新ＦＡ経由でトンネルを介して送受信しながら、新ＦＡに関するモバイルＩＰ登録を行う。この正式登録の開始は遅らせても良い。この様に、後登録ハンドオフによると、新ＦＡでのサービスの確立を早くすることが出来る。

【００１０】インターネットドラフト「モバイルＩＰｖ６における素早いハンドオフ：ｄｒａｆｔ－ｉｅｔｆ－ｍｏｂｉｌｅｉｐ－ｆａｓｔ－ｍｉｐｖ６－０３．ｔｘｔ」は、モバイルＩＰｖ６用にハンドオフ遅延を少なくする類似の技術を提案している。

【００１１】

【非特許文献】シー・パーキンス（Ｃ．Ｐｅｒｋｉｎｓ）編、「ＲＦＣ２００２」、インターネット技術標準化委員会（ＩＥＴＦ：Ｔｈｅ　Ｉｎｔｅｒｎｅｔ　Ｅｎｇｉｎｎｅｒｉｎｇ　Ｔａｓｋ　Ｆｏｒｃｅ）、１９９６年１０月

【００１２】

【発明が解決しようとする課題】後登録ハンドオフと前登録ハンドオフの両方の方法共、Ｌ２トリガは、タイミング良く発せられると仮定されている。Ｌ２トリガは、Ｌ２ハンドオフプロセスに結びついたイベントが起きた、もしくは起こりそうであるということを表している通知のいわば総称である。このようなイベントの１つとして、ＭＮのＬ２接続点の変更があると言うことを知らせる早期通知がある。他のイベントとしては、ＭＮの旧Ｌ２アクセスポイントとの接続が失われたこと、新Ｌ２アクセスポイントとの接続が確立したことなどがある。普通、サブネットワーク内にいる無線アクセスネットワーク（ＲＡＮ）または無線ネットワークコントローラ（ＲＮＣ）の補助により、Ｌ２トリガが発せられる。ここでこのサブネットワークでは、そのサブネットワーク内にいるＭＮ全ての位置情報を常に把握して保持している。従って、素早くタイミングの良いＬ２トリガを発するには、ＭＮが移動する２つの隣接するＲＡＮ間の密接な協力が必要となる。２つのＲＡＮ間の密接な協力は、この２つのＲＡＮが同じ無線アクセス技術を使用しているときに限り可能である。よって、Ｌ２トリガを発することに関する前述の仮定は事実上、ＭＮが移動している２つの隣り合うＲＡＮは同じ無線アクセス技術を使用しているという仮定となる。しかしながら、無線ネットワークにおける現在の傾向から、将来の無線ネットワークは、異なる無線アクセス技術を使用している、様々な異なるＲＡＮからなるであろうことを示している。提案されている前登録ハンドオフプロトコルおよび後登録ハンドオフプロトコルは、そのような異種間ハンドオフに対応していない。

【００１３】

【課題を解決するための手段】本発明は、標準ＩＰ登録に関連したハンドオフ遅延を最小にするトンネリングハンドオフプロセスを提供する。本発明は、モバイルＩＰｖ４とＩＰｖ６の両方に適用することができる。よって、本明細書において、モバイルＩＰｖ４で使われる「エージェント」と言う語と、モバイルＩＰｖ６で使われる「アクセスルータ」または「ルータ」と言う語とは交換可能である。さらに、「エージェント」と「ルータ」と「アクセスルータ」と言う語は合わせて、本出願において、「モビリティサービス提供ノード」と言う。

【００１４】本発明は、モバイルノードがあるモビリティサービス提供ノード（ソース）によるあるサブネットを離れ、他のモビリティサービス提供ノード（ターゲット）による他のサブネットに入る状況を考えている。本発明の一実施形態では、モバイルノードは、トリガされたら、２つのモビリティサービス提供ノード間（すなわちソースとターゲット）にトンネルを確立するために、本発明によるトンネリングハンドオフプロセスを開始する。モバイルノードがターゲットノードによる新たなサブネットに入ったら、標準モバイルＩＰ登録プロセスを後回しにする。かわりに、モバイルノードは、自身がターゲットノードによるサブネットにいる間、トンネルを使用してソースノードと通信する。つまり本発明におい

て、モバイルノードがソースノードからターゲットノードへのＬ２ハンドオフを終えた後で、Ｌ３ハンドオフかターゲットノードに関するＩＰルーティング更新を行う前には、ソースノードとターゲットノードとの間に確立されたトンネルを使用して、モバイルノードはソースノードと通信する。モバイルノードがソースノードとターゲットノードとの間でＬ２ハンドオフを行う前か後に、トンネルが確立されても良い。

【００１５】一実施形態において、モバイルノードは、トリガされるとすぐに本発明によるトンネリングハンドオフプロセスを開始するエンティティである。トリガは、モバイルノードの外部で生成されても内部で生成されても良い。また、本発明のハンドオフプロセスを開始するのに、モバイルノードは、内部のＬ２かＬ３の信号を使用しても良い。ソースノードとターゲットノードが同じ無線アクセス技術を使用しているかどうかにかかわらず、モバイルノードは、本発明によるトンネリングハンドオフを開始することができる。

【００１６】本発明の他の実施形態においては、モバイルノードはトリガされるとすぐに、モバイルノードがソースノードからターゲットノードへのＬ２ハンドオフを始める前にトンネルを確立するために、トンネリングハンドオフ要求をソースノードに送信する。モバイルノードは、Ｌ２アドレスのようなターゲットノードのＬ２識別子を取得して、トンネリングハンドオフ要求に含める。ソースノードは、近隣のネットワークのＬ３アドレスやＩＰアドレスのようなＬ３識別子を、そのネットワークのＬ２識別子に関連付けたテーブルを、前もって作成しておき、モバイルノードからのトンネリングハンドオフ要求の中のＬ２識別子に対応するＬ３識別子を、テーブル中に調べるようにしても良い。モバイルノードは、可能なら、ターゲットノードのＬ３識別子を取得して、トンネリングハンドオフ要求内にＬ３識別子を入れても良い。

【００１７】また、モバイルノードがソースノードからターゲットノードにＬ２ハンドオフをした後、モバイルノードがトンネリングハンドオフ要求をターゲットノードに送信しても良い。また、他の実施形態において、異なる無線アクセス技術を使用しているソースノードからターゲットノードにハンドオフを行なう場合、本発明によるトンネリングハンドオフを開始するのは、モバイルノード、ソースノード、およびターゲットノードのどれでも良い。

【００１８】

【発明の実施の形態】本発明の好適な実施形態を図面を参照しながら説明する。ここで同一の要素は同一の符号で表される。本明細書に開示する以下の好適な実施形態の説明は、例示のためであり発明の範囲を限定しようとするものではない。

【００１９】図１は、本発明の用途先として意図している第３世代無線モバイルアクセスＩＰデータネットワーク１００を例示している図である。本出願で、ＩＰデータネットワーク１００は、ＩＭＴ－２０００標準と無線モバイルアクセスネットワークの為のＩＴＵの仕様に準拠していると仮定する。更に、データネットワーク１００は、ＩＥＴＦのモバイルＩＰｖ４標準に拠ったモバイルＩＰサポートを実装していると仮定する。しかしながら、当業者ならば、本発明は、モバイルＩＰｖ６を実施しているデータネットワークにも適用することができることを理解するであろう。よって、本出願の全般にわたり、「エージェント」と言う語は、「アクセスルータ」または「ルータ」と言う語と交換して使われうる。同じように、「エージェントディスカバリ」は「近隣ディスカバリ」と、「エージェントソリシテーション」は「ルータソリシテーション」と、「登録要求」は「バインディング更新」と、交換して使われうる。特に、「エージェント」と「ルータ」と「アクセスルータ」と言う語は合わせて、本出願において、「モビリティサービス提供ノード」と言う。モバイルＩＰｖ６プロトコルは、「モバイルＩＰｖ６におけるモビリティサポート」という題のドラフト作業書に記載されている。この文書を本明細書に参照として組み込む。

【００２０】無線モバイルアクセスＩＰネットワーク１００は、固定接続点またはリンクなどの多くの固定ノード（図示せず）を有するＩＰデータネットワーク１２０をそのコアとして有している。ＩＥＴＦによるＲＦＣ２００２で規定されているインターネットプロトコル・バージョン４（ＩＰｖ４）に従って、デジタルデータはネットワーク内やネットワークを越えて伝送される。なお、ＩＰｖ４は、通信プロトコルの例であり、ＩＰｖ６のような他の通信プロトコルに換えても良い。コアネットワーク１２０のノードのうちいくつかは、通常のルータ（図示せず）であり、通常のインターネットのアドレス・ルーティングプロトコルに従って、パケットを、ネットワークにつながっているソースノードと宛先ノードとの間でルーティングする。

【００２１】コアネットワーク１２０上には、ゲートウェイルータ１３０の集合があり、ＩＰモバイルバックボーン１４０を形成している。ＩＰモバイルバックボーンを形成しているゲートルータ１３０は、それ自身がコアネットワーク１２０のノードであり、コアネットワーク１２０を超えてお互いに通信を行う。各ゲートウェイルータ１３０には、複数のエージェント１４５がつながっていて、モバイルノード１３５と通信をすることができる。モバイルノードは、セル式ハンドセット、セル式電話、ハンドヘルドコンピュータ、パーソナル情報機器のような無線通信デバイスであり、数はいくつあっても良い。エージェント１４５は、ホームエージェント（ＨＡ）およびフォーリンエージェント（ＦＡ）として機能するモビリティサービス提供ノードであり、ＩＥＴＦの

RFC2002に規定されているように、ゲートウェイ130を介してコアネットワーク120へモバイルノード135を接続する。エージェント145は、レイヤ3アクセスネットワークエンティティである。モバイルノード135は、無線アクセスポイント（AP）155を介して、エージェント145と通信する。AP155は、レイヤ2アクセスネットワークエンティティである。AP155が複数でサブネットワーク150を形成している。エージェント145の各々は、サブネットワーク150にサービスを提供し、サブネットワーク150とデータネットワーク100との間のインターフェースとして、ネットワークリンクを提供する。モバイルノード135とAPは、CDMA、W-CDMA、または類似のデジタルデータ通信技術を使用して、お互いに通信を行う。

【0022】RFC2002に従って、モバイルノードの各々にはホーム無線サブネットワークが割り当てられている。このホーム無線サブネットワークはホームエージェント145を有している。このホームエージェント145は、モバイルノードの現在地情報を持っていて、モバイルノード宛のパケットをモバイルノードが現在いる地点に転送する。他のエージェント145は、フォーリンエージェントとして働き、ここにモバイルノードが、ホームサブネットワークから離れている時に「訪れる」ことができる。ある時点でモバイルノード135が通信している相手が、ホームエージェントであってもフォーリンエージェントであっても、そのエージェントは、ネットワークリンクを確立してモバイルノードにネットワークアクセスを提供する。モバイルノードとエージェントの各々は、通常のインターネットプロトコルを使用している通常の固定ノード式データネットワークと同じように、固有のIPアドレスを有している。

【0023】データネットワーク100中では、2レベルのハンドオフプロセスが考えられている。最初のレベルのハンドオフは、マクロレベルハンドオフ、またはレイヤ3（L3）ハンドオフであり、モバイルノードが、あるエージェント配下の無線サブネットワークから他のエージェント配下のサブネットワークへ接続点を変更するような、モバイルノードの位置の変化が関係する。この様に、L3ハンドオフの間に、モバイルノードのネットワークリンクが必ず変わる。もう1つのレベルは、マイクロレベルハンドオフ、またはレイヤ2（L2）ハンドオフであり、モバイルノードが同一のAPネットワーク150内で位置を変更することに関していて、モバイルノードのネットワークリンクは変わらず、モバイルノードの無線リンクが変更になる。L2ハンドオフは無線セル方式通信ネットワークにおいて標準なものである。例えば、近隣のAPへの到達可能性を判定するのに、近隣のAPからのビーコン信号の強度を使うのことが良く知られている。

【0024】図2は、標準モバイルIPレイヤ3ハンドオフプロセスを簡略に示した図である。ネットワーク120はIPデータネットワークであり、IPv4を実装している。ネットワーク120にゲートウェイ（図示せず）を介して接続しているのは、モビリティエージェント145（HA、FA1、FA2、およびFA3）である。上述のように、このモビリティエージェントの各々は、サブネット150を作っていて、そのサブネット内にAP155（図示せず）が複数含まれている。各サブネットワークは、無線アクセスネットワーク（RAN）または無線ネットワーク制御装置（RNC）を有していて、このRANまたはRNCは、サブネット内に位置するMN全ての位置情報の状況を常に把握している。

【0025】MN135は現在、FA1配下のサブネットワーク内の開始位置Aにいて、中間位置Bを経由して位置Cに移動しようとしている。MNは、HA配下のサブネットに最初いたので、HAから与えられたホームIPアドレスをずっと使うことになる。しかし、HAのサブネットから離れたFA1のサブネット内に現在いるので、MNは、一時的にFA1から与えられた気付アドレスによってアドレス指定される。MNは以前にFA1に関してモバイルIP登録プロセスを行ったので、HA内にこの気付アドレスがバインディング情報として登録されている。従って、MN宛のデータは、HAが途中で受け取り、FA1にトンネル転送されて、FA1からMNに転送される。MNからのデータは、HA経由にしても、宛先に直接送っても良い。

【0026】MNが開始位置Aから中間位置Bの方へ移動するにしたがい、FA1からの無線が届かなくなる位置が来る。MNはFA1配下のサブネットワーク150を出て、FA2配下のサブネットワーク150に入る。MNが中間位置Bを過ぎると、L2トリガが発せられ、MN、FA1、FA2にMNのL2ハンドオフがすぐに起こるとの通知がされる。トリガは、MNがFA1とのリンクを失う充分前に発せられる。これはMNがFA1とのリンクを失う前にFA2へのハンドオフを終えることができるようにするためである。L2ハンドオフは、MN、FA1、FA2による協調作業であり、FA1とFA2のRANによって補助される。MNはFA2へのハンドオフを終えると、FA2によるサブネット150内で無線リンクを持つことになる。また、MNがFA2のサブネットに入るとすぐに、MNはFA2からエージェント広告を受信し始める。FA2からのエージェント広告により、MNはFA2配下のサブネット内で現在稼動していると知ることができる。

【0027】MNがさらに目的位置Cへと向かうにつれて、MNは標準L3ハンドオフ、すなわちFA2に関するモバイルIP登録を行う。登録プロセスの始めに、MNはFA2からのエージェント広告から気付アドレスを取り出す。アドレス自動設定の好ましい手順がIETF

のＲＦＣ２４６２に記載されている。この文書を参照として本明細書に組み込む。ＭＮの新たな気付アドレスは、ＦＡ2のＩＰアドレスと、ＦＡ2により送信されていたＭＮ用のサブネットアドレス部分を有している。ＭＮは次に、この気付アドレスとＭＮがしばらく使用するホームＩＰアドレスとを含んだ登録要求をＦＡ２経由でＨＡに送り、新しい気付アドレスを登録する。ＨＡは、これに応答して、自身のキャッシュ内のＭＮのバインディング情報を更新する。そしてＭＮにＦＡ２経由で登録応答を送る。これにより、Ｌ３リンクがＭＮとＦＡ2の間で確立される。これ以降、ＭＮのホームＩＰアドレス宛に送られるパケットは、ＨＡが受け取って、ＦＡ2にトンネル転送され、ＦＡ2からＭＮに送られる。

【００２８】なお、この標準モバイルＩＰ登録の間、ＭＮがデータを送受信できない期間が発生する。この期間、つまりＭＮがＦＡ１との無線通信ができなくなってから、ＦＡ２へのＬ３ハンドオフが終わるまでのことをハンドオフ遅延と呼ぶ。この登録プロセスの間に起こるハンドオフ遅延は、数１００ミリ秒を超えてしまうと計算されている。このハンドオフ遅延の大きな原因は、ＭＮが新しいエージェントを発見することと、ＨＡでの更新処理と、そして恐らく最も大きな原因である、ＨＡとＦＡ２（これらはおそらく他のネットワークを介して分け隔てられている）との間での登録要求と返答メッセージの伝送にかかる時間である。標準モバイルＩＰ登録プロセスによるハンドオフ遅延は、リアルタイム通信や遅延に敏感な通信が許容することができるものより大きくなりうる。

【００２９】本発明は、Ｌ３ハンドオフに関する遅延を少なくする２つの方法を提供する。第１の方法は、プリＬ２ハンドオフモバイル起動トンネリングハンドオフ（Ｐｒｅ－ＭＩＴ）と呼ばれ、図３（ａ）、３（ｂ）、３（ｃ）に詳しく図示されている。第２の方法は、ポストＬ２ハンドオフモバイル起動トンネリング（Ｐｏｓｔ－ＭＩＴ）と呼ばれ、図４（ａ）、４（ｂ）、４（ｃ）に詳しく図示されている。両方の方法とも、トリガモードかトリガレスモードで機能する。図３（ａ）、３（ｂ）、３（ｃ）を参照して、Ｐｒｅ－ＭＩＴを最初に説明する。

【００３０】図３（ａ）は、ＩＰｖ４のためのＰｒｅ－ＭＩＴを図示している。図３（ｂ）は、図３（ａ）に示されるＰｒｅ－ＭＩＴのトリガモードのタイミングを説明する図である。図３（ａ）には、２つのＦＡが図示されている。これらＦＡは、既に述べた様に、それぞれサブネット１５０を有している。このサブネットは、ＡＰ１５５を有している。ＭＮは旧ＦＡ（ソース）に関する登録がされていて、旧ＦＡを介してデータの送受信をしている。ＭＮは現在旧ＦＡによるサブネットを離れ、新ＦＡ（すなわちターゲット）へ向けて移動している。なお、新旧ＦＡは、異なる無線アクセス技術に対応していると仮定する。この仮定は、本発明で説明される他の実施形態でも使われる。しかし、同じ無線アクセス技術に対応したＦＡ間のハンドオフにも、本発明は適用することができる。

【００３１】ＭＮが旧ＦＡと新ＦＡとの間のある点にまで来て、旧ＦＡとのデータ通信が出来なくなりそうになると、ＭＮは、Ｌ２ハンドオフが起こりそうであると通知するＬ２トリガを受信する（ステップ３０１）。Ｌ２トリガと言うのは、なにかイベントが起こるもしくは起こりそうであると言うことを表した、レイヤ２から送られる通知のいわば要約である。本発明において考えられているＬ２トリガには３種類ある。第１のトリガは、Ｌ２ハンドオフが起こりそうであると通知するトリガである。この第１のトリガは、ＭＮ、新旧ＦＡのどれが受信しても良い。第２のトリガは、リンクダウントリガと呼ばれ、ＭＮと旧ＦＡがその間に有していたＬ２の通信リンクが失われたということをＭＮと旧ＦＡに通知する。第３のトリガは、リンク確立トリガと呼ばれ、ＭＮと新ＦＡに、ＭＮと新ＦＡの間に新たなＬ２リンクが確立したということを通知する。

【００３２】本発明においては、Ｌ２トリガは特定のＬ２信号に関連してはいないが、無線リンクプロトコルとして広く利用可能である（もしくは可能であろう）Ｌ２情報に基づいている。よって、トリガは様々な方法で実装されうる。例えば、トリガが生成されたら呼び出されるコールバック関数を、ＩＰスタックが登録することを、Ｌ２ドライバが許可しても良い。オペレーティングシステムが、スレッドにシステムコールを実行させて適切なトリガを生成させても良い。トリガは、トリガ通知とパラメータ情報を、Ｌ２かＬ３で新ＡＰと旧ＡＰとの間を転送するためのプロトコルを含んでいても良い。また、トリガ情報は、ＩＰスタックにとって、帯域外通信として、ドライバからオペレーティングシステムカーネル内で利用可能であっても良い。また、トリガは、もし以下のエンティティがＬ２トリガを生成することができるならば、旧ＦＡ、新ＦＡ、無線アクセスネットワーク（ＲＡＮ）および無線ネットワークコントローラ（ＲＮＣ）のいずれから来るのでも良い。ここでＲＮＣとは、旧ＦＡか新ＦＡによるサブネットにサービスを提供するものである。ＭＮは、トリガを発することができるならば、自身でトリガを発しても良い。

【００３３】Ｌ２ハンドオフが発生しそうであるとのＬ２トリガによってトリガされ、ＭＮはモバイルハンドオフ要求（ＨＲｅｑ（ｍ））を旧ＦＡに送信する（ステップ３０２）。このＨＲｅｑ（ｍ）のメッセージフォーマットは、図５の様に４つのフィールドを有したインターネット制御メッセージプロトコル（ＩＣＭＰ）からなる特別のメッセージフォーマットになっている。ＩＣＭＰの４つのフィールドは、タイプフィールド、コードフィールド、チェックサムフィールド、そして予約フィール

ドである。これらのフィールドはビットで構成されている。タイプフィールドは、メッセージがモバイルハンドオフ要求（ＨＲｅｑ（ｍ））であることを示すフィールドである。コードフィールドは０を値として持っている。チェックサムフィールドは、１６ビットからなり、ＩＣＭＰタイプフィールドからのＩＣＭＰメッセージの１の補数和の１の補数である。チェックサムを計算するために、チェックサムフィールドは０にセットされている。予約フィールドは、３２ビットあり、０にセットされている。

【００３４】この特別なメッセージのフォーマットにある他のフィールドは、アドレスフィールドである。アドレスフィールドには、ビット形式で、ターゲットトリガパラメータが含まれている。ターゲットトリガパラメータは、フォーリンエージェントのリンクレイヤアドレスつまりＬ２識別子（すなわちＬ２アドレス）であり、３つまで入る。ＭＮは、ＦＡから受信したパイロットビーコン信号からこれらのＬ２識別子を取得しても良い。旧ＦＡは、所定のポリシーにより３つのＬ２識別子から１つを選択しても良い。本実施形態において、本発明をよりよく理解する為に、このアドレスフィールドには、１つのアドレスすなわち新ＦＡのアドレスが含まれていると仮定する。また、旧ＦＡは新ＦＡのアドレスを知っていると仮定する。新ＦＡのＩＰアドレスが無ければ、旧ＦＡは新ＦＡと直接通信を行うことができない。旧ＦＡが新ＦＡのアドレスを得る方法として２つある。１つはＭＮから得る方法である。新ＦＡからのエージェント広告がＭＮに着いたときに、ＭＮはこのエージェント広告から新ＦＡのＩＰアドレスを取得して、ＨＲｅｑ（ｍ）に付加する。もう１つは、旧ＦＡに、近隣のＦＡのＩＰアドレスをＬ２識別子と関連つけて、テーブルに保持するように要求することである。ＨＲｅｑ（ｍ）にＩＰアドレスが付加されていないときは、旧ＦＡはＨＲｅｑ（ｍ）の拡張部の１つからＬ２識別子を取り出す。このＬ２識別子から、旧ＦＡは対応するＩＰアドレスをテーブルから探し出す。このテーブルの形式と検索処理は、図３（ｃ）に示されたＰｒｅ－ＭＩＴトリガレスモードの説明のところで詳細に説明する。本実施形態においては、ＭＮからのＨＲｅｑ（ｍ）には、新ＦＡのＬ２とＬ３識別子を含んだ拡張部があると仮定する。

【００３５】ＭＮからＨＲｅｑ（ｍ）を受信すると、旧ＦＡは、ＨＲｅｑ（ｍ）に付加されている拡張部の１つに含まれているＬ３識別子を取り出し、ＭＮが旧ＦＡから新ＦＡに接続点を変更しようとしていると判定する。旧ＦＡは、それから新ＦＡにソースエージェントハンドオフ要求（ＨＲｅｑ（ｓ））を送信する（ステップ３０３）。旧ＦＡからＨＲｅｑ（ｓ）を受信すると、新ＦＡは、その要求に付加されている拡張部を開けて、ＭＮが旧ＦＡから新ＦＡにハンドオフしようとしていることを知る。これに応答して、新ＦＡは、旧ＦＡにハンドオフ応答（ＨＲｐｌｙ（ｔ））を送り返す（ステップ３０４）。これにより、新旧ＦＡ間にトンネルが確立する。これらのトンネルは単方向で、新ＦＡから旧ＦＡへのデータ転送のみに使用されても良い。もしくは、トンネルは双方向で、新旧ＦＡ間のデータ交換に使用されても良い。新ＦＡからのハンドオフ返答は、旧ＦＡによりＭＮに転送される（ステップ３０５）。

【００３６】ＨＲｅｑ（ｓ）とＨＲｐｌｙ（ｔ）は、同じビットフォーマットをもった特別なメッセージである。図6は、ＨＲｅｑ（ｓ）とＨＲｐｌｙ（ｔ）のメッセージフォーマットを示している。このフォーマットでは、タイプフィールド、Ｈビット、Ｎビット、Ｒビット、Ｍビット、Ｇビット、Ｔビット、Ｂビット、生存期間フィールド、ＭＮのホームアドレスフィールド、ＨＡのホームアドレスを有している。本発明に関係する部分を以下に説明する。タイプフィールドの値は、メッセージがハンドオフ要求（ＨＲｅｑ）であるかハンドオフ応答（ＨＲｐｌｙ）であるかを示す。Ｈビットは、ソースがトリガされたことによるハンドオフ要求であることを示す。Ｈビットがセットされていて、Ｎビットがセットされていない時、この要求がソースからであることを示している。Ｎビットは、ターゲットトリガされたことによるハンドオフ要求であることを示す。Ｎビットがセットされていて、Ｈビットがセットされていない時、この要求がターゲットからであることを示している。本実施形態においては、旧ＦＡがＨＲｅｑを送信している。よって、Ｈはセットされていて、Ｎはセットされていない。ＨかＮの両方共セットされていない時で、要求がトンネルを更新するための要求であるなら、Ｒビットはセットされている。Ｔビットは、旧ＦＡは、順方向と逆方向トンネルサービスの両方共に対応するのにすすんで応じることを示している。このように、旧ＦＡは、トンネルを単方向にするか双方向にするかの一致したポリシーを決めても良い。Ｂビットは、ＭＮがＨＡへの逆方向トンネルを要求していると言うことを示しているとともに、新ＦＡが旧ＦＡに逆方向トンネリングを行っていなければ、新ＦＡがＨＡへの逆方向トンネルを使用すべきであるという事を示している。

【００３７】生存期間フィールドは、ＭＮへのトンネルサービスがどのくらい保たれるのかを秒で示している。生存期間フィールドの値が０にセットされている場合で、Ｔビットがセットされていないなら、旧ＦＡはＭＮへはどのパケットもトンネル転送しない。生存期間フィールドの値に正の値が入っていて、Ｔビットがセットされていたら、旧ＦＡは、示された時間トンネル転送を行う。識別子フィールドは、６４ビットあり、登録要求を登録応答に照合するのに使用する、また登録メッセージの応答攻撃に対する守りに使用する。

【００３８】旧ＦＡとＭＮとの間にＬ２リンクが残っている限り、旧ＦＡは、ＭＮのＨＡから来たデータをＭＮ

にトンネル転送し、そしてＭＮから来たデータを、ＨＡにトンネル転送し返すか、直接宛先に送る。ＭＮとの間のＬ２リンクが失われたらすぐに、リンクダウントリガにより知らされた旧ＦＡは、旧ＦＡと新ＦＡとの間に確立したトンネルを使用して、ＭＮ宛のデータを送り始める。ＭＮが新ＦＡによるサブネットに入り、ＭＮと新ＦＡとの間のＬ２リンクが確立するとすぐに、新ＦＡは、リンク確立トリガによって知らされて、旧ＦＡから来たデータをＭＮにトンネル転送する。この時、トンネルが双方向のものであれば、新ＦＡは、ＭＮからのデータを旧ＦＡにトンネル転送しても良い。

【００３９】このように、本発明の実施形態によれば、ＭＮはＬ２トリガを利用して、新旧ＦＡ間にトンネルを確立し、ＭＮはこのトンネルを使用して、新ＦＡによるサブネット上にいるときも、旧ＦＡを使用してデータ通信を続けることが出来る。これによって、ハンドオフ遅延の原因となる要素をなくす事が出来、リアルタイムアプリケーションに対する影響を最小にしながら、新たな接続点での素早いサービス開始を実現する事が出来る。ＭＮは、新ＦＡとのＬ２通信が確立した後、図２に示されるような正式なモバイルＩＰ登録を最後には行わなければならないが、しかしこれは、ＭＮからの要求によって後に行っても良い。ＭＮが登録を行うまで、新ＦＡと旧ＦＡは、ＭＮに切れ目のない接続を提供するために、要求されたように、トンネルを確立したり移動したりする。

【００４０】図３（ｃ）は、トリガレスモードにおけるＰｒｅ－ＭＩＴ処理のタイミングを示した図である。トリガレスモードにおいては、旧ＦＡは、近隣のＦＡのＩＰアドレスとＬ２識別子を有しているテーブルを有している。これらのアドレスは、ＲＦＣ２００２のモバイルＩＰｖ４で規定されているルータソリシテーションとルータ広告を使用して、前もって取得されている。本発明とＲＦＣ２００２との差は、ＲＦＣ２００２においては、これらのプロトコルは、ＭＮと近隣ＦＡとの間において実施されているが、本発明では、同じプロトコルが、ＦＡとその近隣のＦＡとの間において実施されているということである。このように、本発明においては、旧ＦＡは、近隣のＦＡに前もってエージェントソリシテーションを送信する。これに応答して、近隣のＦＡは旧ＦＡにエージェント広告を送信し返す。旧ＦＡは、次に、この広告に付加されている拡張部からＬ３とＬ２の識別子を取り出し、旧ＦＡ内部のテーブルにキャッシュする。

【００４１】また、トリガレスモードにおいては、Ｐｒｅ－ＭＩＴを開始するのにＭＮが使えるＬ２トリガはないということが仮定されている。よって、ＭＮは、自身の内部のＬ２信号を使用してＰｒｅ－ＭＩＴを開始しなければならない。もしＭＮのＬ２において、リンク評価機能があり、それがリンクの質低下を認めたら、ＭＮのＬ３にハンドオフを通知することができる。普通、ＭＮのＬ２は、ＭＮが通信している相手と近隣のＦＡからのパイロットビーコン信号の強度をモニターすることが出来る。ビーコン信号の強度をモニターすることで、Ｌ２がＬ３にＬ２ハンドオフが起こりそうであると通知することが出来る。Ｌ２は、また、Ｌ３への通知で、優先付けられた見込み新候補ＦＡとそのＬ２識別子を提供する事が出来る。また、ＭＮは、Ｌ２ハンドオフを予測するために、パケット遅延のＬ３評価を使用してもよい。このような、パケット遅延を基にしたハンドオフ予測は、特願平２００２－１９０７６「無線の移動体アクセスデジタルネットワークにおけるモビリティ予測方法」、また特願平２００２－１９０８４「モビリティ予測を用いた無線の移動体アクセスのディジタルネットワークにおける高速動的ルート設定」に記載されている。

【００４２】図３（ｃ）に戻り説明を続ける。ＭＮは旧ＦＡに接続している間、次のハンドオフのための候補ＦＡを見つけるために、旧ＦＡと他の近隣のＦＡからのパイロットビーコン信号をモニターする。ＭＮが旧ＦＡから新ＦＡへと移動している時に、ＭＮは自身のＬ２から、旧ＦＡからのパイロット信号が弱まっているとの通知を受ける。Ｌ２からのこの通知をトリガとして利用して、ＭＮはＰｒｅ－ＭＩＴを開始する（ステップ３０１）。この時、Ｌ２は、受信したパイロットビーコン信号の強度に基づいて、新ＦＡが次のハンドオフのターゲットであるということを、既にＭＮに通知していると仮定する。このＰｒｅ－ＭＩＴを開始したとき、ＭＮは、エージェントソリシテーションに新ＦＡのＬ２識別子を付加して、旧ＦＡに送る（ステップ３０２）。

【００４３】ＭＮからエージェントソリシテーションを受信すると、旧ＦＡは拡張部を開いて、そこからＬ２識別子を取り出す。旧ＦＡは、それからその受信したＬ２識別子に対応するＩＰアドレスをテーブル内に探して、新ＦＡのＩＰアドレスを決定する。そして旧ＦＡは、ＨＲｅｑ（ｓ）を新ＦＡに送信する（ステップ３０３）。このＨＲｅｑ（ｓ）と、次のステップ３０４で送信されるＨＲｐｌｙ（ｔ）は、図６に示される同じデータフォーマットを有している。図３（ｃ）のステップ３０４とステップ３０５で行なわれる処理は、図３（ｂ）の対応するステップで行なわれる処理と同じである。よって、これらの詳しい説明は省略する。トリガレスモードにおいては、ＭＮは、他のＩＰエンティティの補助なしにＰｒｅ－ＭＩＴを開始することができる。このように、トリガレスモードは、異なるアクセス技術を使用しているＦＡ間でハンドオフを行う状況に適する。ネットワーク技術の中には、ネットワーク側において、上述したようなＬ２トリガを利用できないものがある（例えば、ＩＥＥＥ８０２．１１ｘとブルートゥース（登録商標））。本発明によれば、トリガレスモードで稼動しているモバイルノードは、ネットワークがどのようなアクセス技術

を使用していても、異なるネットワーク間におけるＰｒｅ－ＭＩＴを開始することができる。

【００４４】図４（ａ）に、本発明におけるＰｏｓｔ－Ｌ２ハンドオフモバイル起動トンネリングハンドオフ（Ｐｏｓｔ－ＭＩＴ）を示す。図４（ｂ）は、Ｐｏｓｔ－ＭＩＴのトリガモードのタイミングを表す図である。図４（ｃ）は、Ｐｏｓｔ－ＭＩＴのトリガレスモードのタイミングを表す図である。Ｐｒｅ－ＭＩＴとＰｏｓｔ－ＭＩＴの差は、Ｐｒｅ－ＭＩＴは、ＭＮが新ＦＡのサブネット内にいて、旧ＦＡとのＬ２接続を有しているときに開始させられるのに対し、Ｐｏｓｔ－ＭＩＴは、ＭＮが新ＦＡのサブネットに入った後（旧ＦＡとのＬ２接続を失っている）で、新ＦＡへのＬ２接続を確立した後に、開始させられることである。つまり、Ｐｒｅ－ＭＩＴでは、ＭＮが、旧ＦＡから新ＦＡにＬ２ハンドオフを行う前、旧ＦＡ内によるサブネット内にいるときに、新旧ＦＡ間のトンネルが確立する。これに対し、Ｐｏｓｔ－ＭＩＴでは、ＭＮが新ＦＡによるサブネットに入り、新ＦＡへのＬ２ハンドオフが終わった後に、トンネルが確立する。この様に、Ｐｒｅ－ＭＩＴは、トンネルが予測されたＬ２ハンドオフに基づいて確立するので、予測的である。Ｐｏｓｔ－ＭＩＴは、新フォーリンエージェントへのＬ２接続が確立した後に、トンネルが確立するので、応答的である。

【００４５】ＭＮが新ＦＡによるサブネットに入った時に、図４（ｂ）に示されているＰｏｓｔ－ＭＩＴが開始する。ＭＮが旧ＦＡによるサブネットを出る時、ＭＮは、Ｌ２ハンドオフが起こりそうだと知らせるＬ２トリガを受信する。しかし、ＭＮは、このトリガを無視し、Ｌ２ハンドオフを起こさせる。ＭＮが新ＦＡによるサブネットに入るとすぐに、Ｌ２接続がＭＮと新ＦＡとの間に確立する。ＭＮは、リンク確立トリガにより通知を受け（ステップ４０１）、Ｐｏｓｔ－ＭＩＴを開始する。または、ＭＮは、新ＦＡに関して標準モバイルＩＰ登録を行っても良い。ＭＮが標準登録プロセスを行うなら、登録プロセスが終わるまでＭＮが送受信できなくなる期間がハンドオフ遅延に加わる。旧ＦＡへのＬ３接続が失われた時に、遅延に敏感なデータの送受信をＭＮが行っているのであれば、ＭＮは、本発明によるＰｏｓｔ－ＭＩＴを行うべきである。

【００４６】リンク確立トリガによって起動して、ＭＮは、新ＦＡにＨＲｅｑ（ｍ）を送る（ステップ４０２）。このＨＲｅｑ（ｍ）のデータフォーマットは、図５に既に示したものである。違いは、Ｐｒｅ－ＭＩＴにおいて使用されるＨＲｅｑ（ｍ）は、新ＦＡのＬ２識別子（Ｌ３識別子は、オプションである）を有した拡張部を有しているが、Ｐｏｓｔ－ＭＩＴにおいて使用されるＨＲｅｑ（ｍ）は、旧ＦＡのＩＰアドレスを有した拡張部を有している。ＨＲｅｑ（ｍ）を受信すると、新ＦＡは、ＨＲｅｑ（ｔ）を旧ＦＡに送信する（ステップ４０３）。すると、旧ＦＡは、ＨＲｐｌｙ（ｓ）を返す（ステップ４０４）。新旧ＦＡ間でＨＲｅｑ（ｔ）とＨＲｐｌｙ（ｓ）の交換を行うことで、新旧ＦＡ間にトンネルが確立される。トンネルが確立したとＭＮに通知するために、旧ＦＡからのＨＲｐｌｙ（ｓ）は、新ＦＡからＭＮに転送される（ステップ４０５）。トンネルを通してＭＮへ最初のデータが送られるときに、旧ＦＡからのＨＲｐｌｙ（ｓ）がＭＮに転送されるようにしても良い。ＨＲｅｑ（ｔ）とＨＲｐｌｙ（ｓ）は、図６に示されたようなメッセージフォーマットをしている。ＨＲｅｑ（ｔ）は新ＦＡから旧ＦＡへと送信されるので、ＨＲｅｑ（ｔ）のＨビットはセットされず、Ｎビットはセットされる。ＨＲｅｑ（ｔ）のＴビットがセットされていたら、新ＦＡは逆方向トンネルサービスを要求していることになる。また、生存期間フィールドで示される期間は、新ＦＡが要求している逆方向トンネルを生存させる期間である。生存期間の値が０である時は、新ＦＡは逆方向トンネルを要求していないことを示している。

【００４７】新旧ＦＡ間のトンネルを使用して、新ＦＡのサブネット内にＭＮがいても、旧ＦＡからデータを受信することが出来る。Ｐｏｓｔ－ＭＩＴにおいては、ＭＮがリンク確立トリガを受信してからトンネルが新旧ＦＡ間に確立されるまで、ＭＮはデータを受信することが出来ない。しかしながら、ＭＮがモバイルＩＰ登録プロセスを行うときにおける、登録要求と応答メッセージがＭＮとＨＡとの間をネットワークを通して伝送することにかかる時間と比べると、新旧ＦＡ間にトンネルを確立するのにかかる時間は短い。よって、Ｐｒｅ－ＭＩＴのように、Ｐｏｓｔ－ＭＩＴによれば、ハンドオフ遅延を遅らせる要因を取り除くことができる。そして、新たな接続点において素早いサービス開始が可能になる。ＭＮは、結局Ｌ３ハンドオフを行わなければならないが、ＭＮの要求にしたがい、後に遅らせることが出来る。

【００４８】図４（ｃ）は、トリガレスモードでＰｏｓｔ－ＭＩＴを行う場合のタイミングを表す図である。トリガレスモードでのＰｒｅ－ＭＩＴの場合と同じように、ＭＮがＰｏｓｔ－ＭＩＴを開始するのに、Ｌ２トリガは利用できない。よって、Ｐｏｓｔ－ＭＩＴを開始するのに、ＭＮは、自身の内部のＬ２信号を使用しなければならない（ステップ４０１）。このために使用可能なＭＮ内部のＬ２信号として、ＭＮのリンク層のプロトコルスタックにより生成され、ＭＮのデバイスドライバで利用可能な変換情報を使用してＩＰインターフェースへＡＰＩを介して上がってくる内部リンク確立通知とリンクダウン通知がある。トリガモードで使用されるリンク確立トリガやリンクダウントリガと違い、これらのリンク確立・リンクダウン通知には、ＭＮが接続している（もしくは接続していた）ＡＰのＬ２とＬ３の識別子は含まれていない。例えば、無線ＬＡＮ（ＩＥＥＥ８０２．１１ｂ）において、無線ＬＡＮのコントロールフレ

ームにある脱アソシエーションメッセージか再アソシエーションメッセージを、無線ＬＡＮのデバイスドライバが受信したら、内部のリンク確立とリンクダウン通知が生成されても良い。

【００４９】内部のＬ２信号によりトリガされ、ＭＮは、新ＦＡに、旧ＦＡのＩＰアドレスを拡張部に有したエージェントソリシテーションを送信する（ステップ４０２）。この後のステップ４０３、４０４と４０５において行なわれる処理は、図４（ｂ）で対応する処理と同じである。異なるアクセス技術を使用している異なったネットワーク上でＰｏｓｔ－ＭＩＴが行なわれる状況において、このトリガレスモードは特に有効である。

【００５０】本発明は、モバイルＩＰｖ６を使用したネットワークで使用しても良い。図７（ａ）と７（ｂ）は、モバイルＩＰｖ６用のＰｒｅ－Ｌ２ハンドオフモバイル起動トンネリングハンドオフ（Ｐｒｅ－ＭＩＴ）の図と、そのタイミング図である。既に説明したＩＰｖ４用の基本プロトコルと、モバイルＩＰｖ６用の基本プロトコルに差はない。差は、ハンドオフ処理を実施するのに使われるＬ３メッセージに主にある。ＩＰｖ４用のＰｒｅ－ＭＩＴと同じように、ＩＰｖ６用のＰｒｅ－ＭＩＴでは、旧アクセスルータ（旧ＡＲ）から新アクセスルータ（新ＡＲ）へのＬ２ハンドオフが行なわれる前に、旧ＡＲと新ＡＲとの間にトンネルを確立される。この様に確立されたトンネルにより、ＭＮは、新ＡＲのサブネット内にいる間も、旧ＡＲを使用してデータ通信を行うことができる。これにより、ハンドオフ遅延を遅らせる要因を取り除くことができる。そして、リアルタイムアプリケーションへ影響を与えずに、新たな接続点において素早いサービス開始が可能になる。

【００５１】ＩＰｖ４用のＰｒｅ－ＭＩＴと同じように、ＩＰｖ６用のＰｒｅ－ＭＩＴは、トリガモードとトリガレスモードの両方で機能する。モバイルＩＰｖ６は、モバイルＩＰｖ４以上に、Ｌ２から独立した設計となっている。しかし、Ｌ２ハンドオフが起こりそうであると通知するＬ２トリガが、ＩＰｖ６ネットワークにおいて利用可能であるならば、このＬ２トリガを使用して，ＭＮに本発明のＰｒｅ－ＭＩＴを開始させても良い。Ｌ２トリガがネットワークで利用可能でないなら、トリガレスモードでＰｒｅ－ＭＩＴが行なわれるべきである。トリガレスモードにおいては、ＭＮのＬ２がリンクを評価することが出来るならば、ＭＮは、リンクの質低下を通知するＬ２からの信号を使用しても良い。また、Ｌ２ハンドオフを予測するのに、パケット遅延のＬ３評価を使用しても良い。

【００５２】ＩＰｖ４用のＰｒｅ－ＭＩＴを実装するときに要求されるように、ＩＰｖ６用のＰｒｅ－ＭＩＴを実装するときに、新ＡＲのＬ２識別子とＬ３識別子の両方または片方が要求される。ＭＮは、新ＡＲからのビーコン信号からＬ２識別子を知ることが出来る。また、ＭＮに新ＡＲからのルータ広告が届くならば、ＭＮは、そのルータ広告からＬ３識別子を知ることが出来る。旧ＡＲはＭＮの代わりに、近隣のＡＲにルータ広告を要請するために、前もってルータソリシテーションを送信しても良い。旧ＡＲは、ルータ広告を受信すると、テーブル内に、近隣のＡＲのＬ３識別子をＬ２識別子と関連付けて格納する。ＭＮが旧ＡＲに、新ＡＲのＬ２識別子のみを通知した時、このテーブルが使用されて、新ＡＲのＬ３識別子が特定される。

【００５３】図７（ａ）と７（ｂ）に戻る。Ｌ２ハンドオフが起こりそうだと内部もしくは外部からの信号によりトリガされて（ステップ７０１）、ＭＮはモバイルハンドオフ起動メッセージＨＩ（ｍ）を用意して、旧ＡＲに送信する（ステップ７０２）。このＨＩ（ｍ）は、ＩＰフィールド、インターネットコントロールメッセージプロトコル（ＩＣＭＰ）フィールド、そしてオプションフィールドがふくまれている特別なメッセージフォーマットをしている。ＩＣＭＰフィールドは、図９に示されている。ＩＰフィールドには、４つの値が入り、これによりハンドオフ起動メッセージ（ＨＩ）を送信側から受信側に送るのに必要なパラメータが提供される。ＩＰフィールドの最初の値は、ソースアドレスである。これは、本発明ではＭＮのホームＩＰアドレスである。第２の値は、宛先アドレスであり、本発明においては、旧ＡＲのＩＰアドレスである。第３の値は、ホップ制限量であり２５５にセットされている。最後の値は、ＩＰｖ６セキュリティプロトコルで要求されている認証ヘッダである。この認証ヘッダは、ＨＩを受信機に正当なものであると保証するのに使用される。

【００５４】ＩＣＭＰフィールドにおいて、タイプフィールドの値は、このメッセージがモバイルハンドオフ起動メッセージ（ＨＩ（ｍ））であるということを示している。コードフィールドの値は０である。チェックサムフィールドは、ＩＣＭＰのタイプフィールドからのＩＣＭＰメッセージの１の補数和の１の補数であり、１６ビットからなる。識別子フィールドにより、メッセージの送信者が示され、本発明ではＭＮである。Ｓビットは０にセットされている。Ｕビットはバッファフラグである。Ｕビットがセットされているとき、ＭＮが新ＡＲによるサブネット内でデータを受信することができるようになるまで、新ＡＲは旧ＡＲからトンネル転送されてきたＭＮ宛のパケットをバッファしなければならない。Ｈビットは、Ｐｒｅ－ＭＩＴフラグであり、セットされている場合、ハンドオフ処理がＰｒｅ－ＭＩＴであることを示している。Ｔビットは、Ｐｏｓｔ－ＭＩＴフラグであり、セットされている場合、ハンドオフ処理がＰｏｓｔ－ＭＩＴであることを示している。Ｒビットは０にセットされている。Ｍビットは、モバイル起動フラグであり、セットされている場合、ＭＮがＭＩＴハンドオフを起動していると示している。予約フィールドは０にセッ

トされている。

【0055】オプションフィールドに格納されるのは5つの値である。第1の値は、MNのリンク層（L2）アドレスである。この値は、到着地側がMNを知ることができる様に、このフィールドに入れられるべきである。第2の値は、新ARのリンク層アドレスである。第3の値は、新ARのIP（L3）アドレスである。Pre-MITを実行するために、新ARのリンク層アドレスかIPアドレスがこのオプションフィールドに入れられていなければならない。これは、MNがハンドオフする新ARの身元を、旧ARに通知するためである。第4の値は、旧ARのIPアドレスであり、後に説明するが、MNがPost-MITを起動する時にMNから新ARに送られる。最後の値は、MNの新しい気付アドレス（CoA）である。MNの気付アドレスは、新ARのIPアドレスを含んでいて、さらに新ARが送信しているMNのためのサブネットアドレス部分を含んでいる。

【0056】図7（a）と7（b）に示されるように、HI（m）が旧ARに送信される（ステップ702）。新ARのL3識別子がHI（m）に含まれていなかったら、旧ARは、HI（m）に含まれている新ARのL2識別子に対応するL3識別子をテーブル内で検索する。旧ARは、次に、ソースハンドオフ起動メッセージHI（s）を用意して、これを新ARに送信する（ステップ703）。HI（s）は、IPフィールド、ICMPフィールド、そしてオプションフィールドを有したフォーマットをしている。ICMPフィールドを図10に示す。IPフィールドにおいて、ソースアドレスは、本実施形態の旧ARのIPアドレスとなっている。これは旧ARがHI（s）を送信しているからである。宛先アドレスは、新ARのアドレスに設定されている。ICMPフィールドの値は、MNから送信されたHI（m）から持ってくる。オプションフィールドには、MNのリンク層アドレス、旧ARに接続していた時に使われた古い気付アドレス、新ARにMNが接続してから使用する新しい気付アドレス、旧ARがトンネルを保つように要求した秒で表されるトンネルの生存期間が含まれている。

【0057】これに応答して、新ARは、ハンドオフ確認メッセージ（HACK）を旧ARに送信する（ステップ704）。これにより、双方向もしくは単方向のトンネルが新旧FA間に確立する。HACKは、IPフィールド、ICMPフィールド、そしてオプションフィールドを持ったデータ形式になっている。ICMPフィールドは、図11に示されている。IPフィールドにおいて、ソースアドレスは新ARのIPアドレスである。宛先アドレスは、旧ARのIPアドレスである。ICMPフィールドにおいて、コードフィールドの値は、新ARがハンドオフを受け付けることが出来ない場合は、128か129か130のどれかに設定される。128は受信機（すなわち旧AR）にとって、送信側（すなわち新AR）が何かしらの理由でハンドオフを受けることが出来ないということを意味している。129は、管理上禁止されているので送信側はハンドオフを受け付けることが出来ないと言うことを意味している。130は、リソースが充分でないので送信側がハンドオフを受け付けることができないという事を示している。オプションフィールドには、秒でトンネルの生存期間が示されている。この期間、送信側（本発明ではすなわち新AR）がトンネルを使用したサービスを提供する。

【0058】新ARからのHACKは、旧ARからMNに転送される（ステップ705）。MNが上述の3つの値をICMPフィールドに見つけたら、MNは、ハンドオフのための新たなアクセスルータ候補を探すために、ルータソリシテーションを送信して、標準モバイルIPv6登録プロセスを行う。MNが旧ARにHI（m）を送ってから、所定期間に旧ARからHACKを受信できなければ、MNは同じように、標準モバイルIPv6登録プロセスを行う。

【0059】図8（a）と8（b）は、モバイルIPv6用のPost-L2ハンドオフモバイル起動トンネリングハンドオフ（Post-MIT）の図と、そのタイミング図である。既に説明したIPv4用の基本プロトコルと、IPv6用のPost-MITの基本プロトコルに差はない。差は、ハンドオフ処理を実施するのに使われるL3メッセージに主にある。IPv4用のPost-MITと同じように、IPv6用のPost-MITにおいては、MNと新アクセスルータ（新AR）とのL2接続が確立した後に、旧ARと新ARとの間にトンネルを確立する。これにより、Post-MITは、ハンドオフ遅延を遅らせる要因を取り除くことができる。そして、新たな接続点において素早いサービス開始が可能になる。

【0060】図8（a）と8（b）に示されるPost-MITは、MNが新FAによるサブネットワークに入り、リンク確立トリガを受信することでMNが開始する（ステップ801）。リンク確立トリガによる開始後、MNはモバイルハンドオフ起動メッセージHI（m）を準備して新FAに送信する（ステップ802）。HI（m）において、IPフィールドには、宛先アドレスとして新ARのIPアドレスが入っている。ICMPフィールドにおいては、Hビットはセットされていず、Tビットはセットされている。新ARのリンク層アドレスとIPアドレス両方または片方の代わりに、旧ARのIPアドレスがオプションフィールドに入っている。MNからHI（m）を受信するとすぐに、新ARはターゲットハンドオフ起動メッセージHI（t）を用意し、旧ARに送信する（ステップ803）。旧ARはHACKを新ARに返す（ステップ804）。これにより、双方向か単方向のトンネルが新旧ARの間に確立する。本実施形態において、HI（t）のIPフィールドには、新AR

のＩＰアドレスが、ソースアドレスとして格納されている。宛先アドレスには、旧ＡＲのＩＰアドレスがセットされている。ＩＣＭＰフィールドの値は、ＭＮから送られてきたＨＩ（ｍ）から取ってくる。オプションフィールドには、トンネルの生存期間が秒で含まれている。この生存期間は新ＡＲがトンネルを保つように要求したものである。

【００６１】本実施形態において、旧ＡＲからのＨＡＣＫ内のＩＰフィールドには、ソースアドレスとして旧ＡＲのＩＰアドレスが格納されている。宛先アドレスは、新ＡＲのＩＰアドレスにセットされている。ＩＣＭＰフィールドにおいて、コードフィールドの値は、新ＡＲがハンドオフを受け付けることが出来ない場合は、１２８か１２９か１３０のどれかに設定される。これらの値は、既に述べたものと同じ意味を有している。オプションフィールドには、秒でトンネルの生存期間が示されている。この期間、送信側（本実施形態ではすなわち旧ＡＲ）がトンネルを使用したサービスを提供する。

【００６２】旧ＡＲからのＨＡＣＫは、新ＡＲからＭＮに転送される（ステップ８０５）。ＭＮが上述の３つの値をＩＣＭＰフィールドに見つけたら、ＭＮは、新ＡＲに関して標準モバイルＩＰｖ６登録プロセスを行う。ＭＮが新ＡＲにＨＩ（ｍ）を送ってから、所定期間にＨＡＣＫを受信できなければ、ＭＮは同じように、標準モバイルＩＰｖ６登録プロセスを行う。

【００６３】本発明の好適な実施形態を説明したが、以上の説明は例示のためであり、本発明を限定しようとするためのものではない。本発明の精神と範囲を決めるのは、均等の範囲を含んだ特許請求の範囲である。例えば、実施形態においては、ＭＮのみがＰｒｅ－ＭＩＴとＰｏｓｔ－ＭＩＴハンドオフの開始者であったが、他のＩＰエンティティ（例えば、旧ＦＡ（旧ＡＲ）、新ＦＡ（新ＡＲ）、そして新／旧ＦＡによるサブネットワーク内に位置する無線アクセスネットワーク）が、本発明のハンドオフを開始しても良い。

【００６４】

【発明の効果】以上説明したように、本発明によれば、ハンドオフ遅延を小さくすることができる。

【図面の簡単な説明】

【図１】　本発明の用途として意図している第３世代無線モバイルアクセスＩＰデータネットワークを例示している図である。

【図２】　標準モバイルＩＰ登録プロセスを簡単に示した図である。

【図３】　（ａ）は、本発明の一実施形態によるＩＰｖ４のためのＰｒｅ－Ｌ２ハンドオフモバイル起動トンネリングハンドオフ（Ｐｒｅ－ＭＩＴ）を示す図であり、（ｂ）は（ａ）に示されるＰｒｅ－ＭＩＴのトリガモードのタイミングを説明する図であり、（ｃ）は（ａ）に示されるＰｒｅ－ＭＩＴのトリガレスモードのタイミングを説明する図である。

【図４】　（ａ）は、本発明の他の実施形態におけるＩＰｖ４のためのＰｏｓｔ－Ｌ２ハンドオフモバイル起動トンネリングハンドオフ（Ｐｏｓｔ－ＭＩＴ）を示す図であり、（ｂ）は（ａ）に示されるＰｏｓｔ－ＭＩＴのトリガモードのタイミングを表す図であり、（ｃ）は（ａ）に示されるＰｏｓｔ－ＭＩＴのトリガレスモードのタイミングを表す図である。

【図５】　本発明の一実施形態で使用されるエージェントソリシテーションメッセージのフォーマットを示す図である。

【図６】　本発明の一実施形態で使用されるＭＩＴ要求メッセージのフォーマットを示す図である。

【図７】　（ａ）は、本発明の他の実施形態によるＩＰｖ６用のＰｒｅ－ＭＩＴを示す図であり、（ｂ）は（ａ）に示されるＰｒｅ－ＭＩＴのタイミングを示す図である。

【図８】　（ａ）は、本発明の他の実施形態によるＩＰｖ６用のＰｏｓｔ－ＭＩＴを示す図であり、（ｂ）は（ａ）に示されるＰｏｓｔ－ＭＩＴのタイミングを示す図である。

【図９】　本発明の一実施形態で使用するモバイルハンドオフ開始メッセージのフォーマットを示す図である。

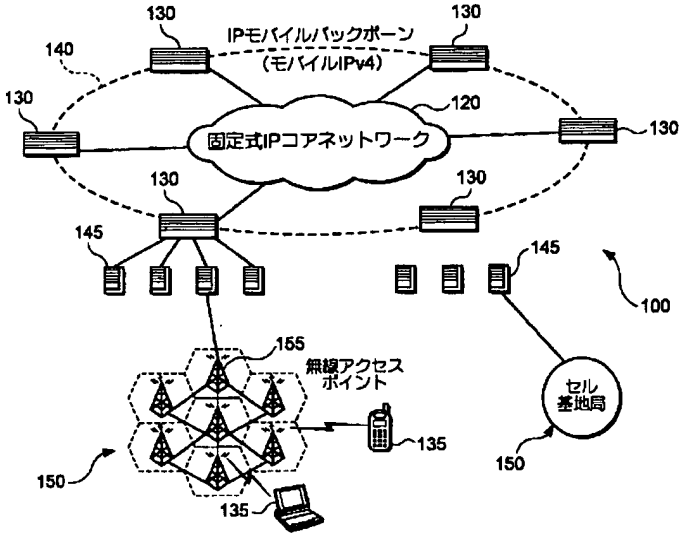
【図１０】　本発明の一実施形態で使用するソースまたはターゲットハンドオフ開始メッセージのフォーマットを示す図である。

【図１１】　本発明の一実施形態で使用するハンドオフ確認メッセージのフォーマットを示す図である。

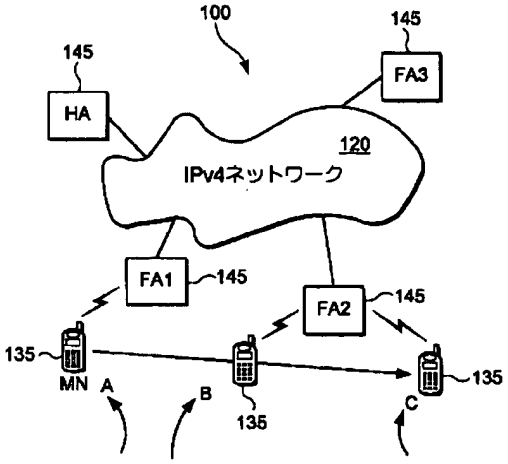
【符号の説明】

１００・・・無線モバイルアクセスＩＰネットワーク、１２０・・・コアネットワーク、１３０・・・ゲートルータ、１３５・・・モバイルノード、１４０・・・ＩＰモバイルバックボーン、１４５・・・サーバ、１５０・・・基地局ネットワーク、１５５、無線アクセスポイント、ＭＮ・・・モバイルノード、ＨＡ・・・ホームエージェント、ＦＡ１、ＦＡ２、ＦＡ３・・・フォーリンエージェント

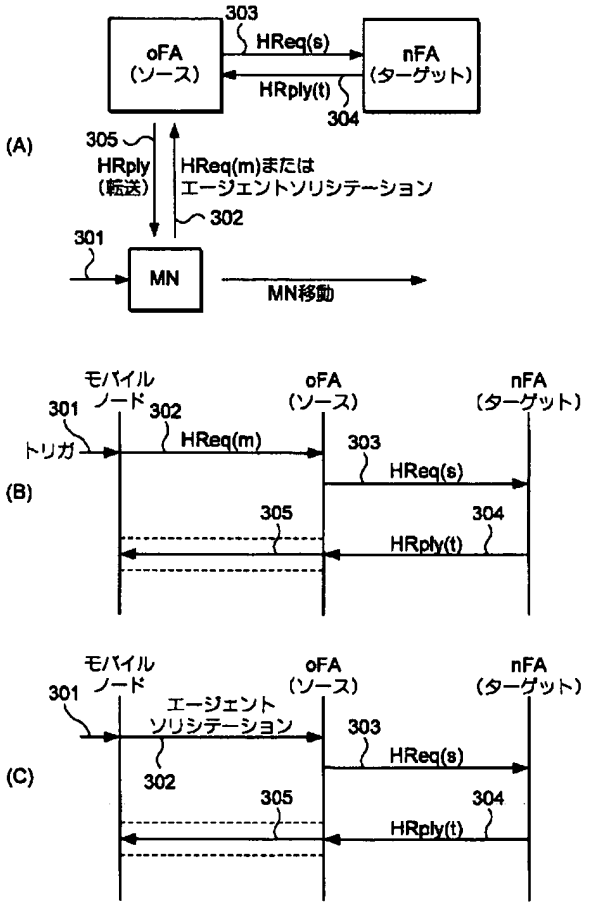
【図1】


130
IPモバイルバックボーン
(モバイルIPv4)
140
120
固定式IPコアネットワーク
145
100
155
無線アクセス
ポイント
135
セル
基地局
150

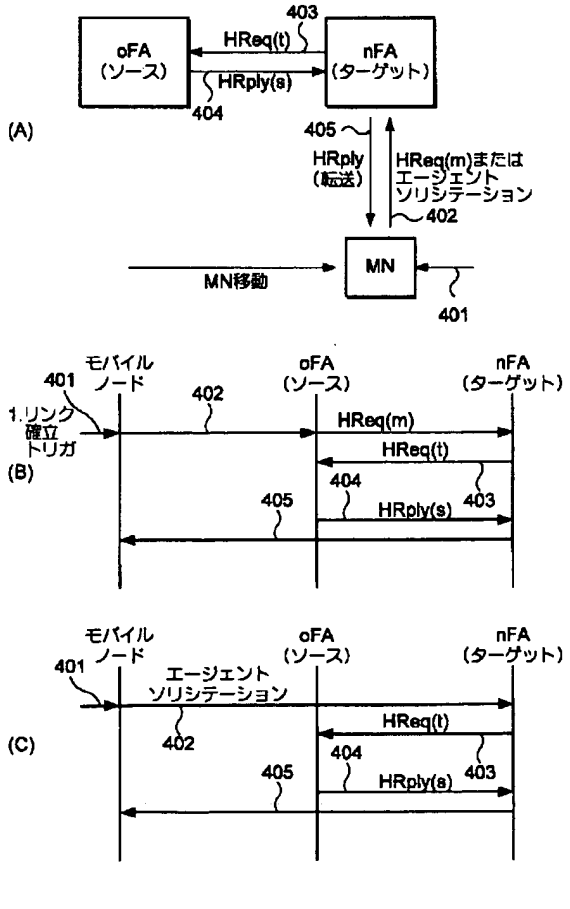
【図2】


100
145
FA3
HA
120
IPv4ネットワーク
FA1
FA2
135
MN
A
B
C

【図3】


303
oFA
(ソース)
HReq(s)
nFA
(ターゲット)
HRply(t)
304
(A)
305
HRply
(転送)
HReq(m)または
エージェントソリシテーション
302
301
MN
MN移動
モバイル
ノード
oFA
(ソース)
nFA
(ターゲット)
トリガ
(B)
(C)
エージェント
ソリシテーション

【図4】


403
oFA
(ソース)
HReq(t)
nFA
(ターゲット)
HRply(s)
404
(A)
405
HRply
(転送)
HReq(m)または
エージェント
ソリシテーション
402
MN
MN移動
401
モバイル
ノード
1.リンク
確立
トリガ
(B)
(C)
エージェント
ソリシテーション

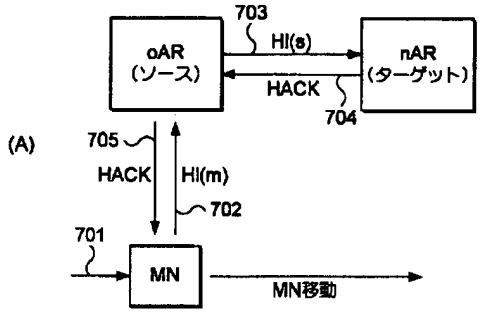
【図5】

タイプ(8)	コード(8)	チェックサム(16)
予約(32)		
ターゲットトリガパラメータ (IPv4アドレス3つまで)		

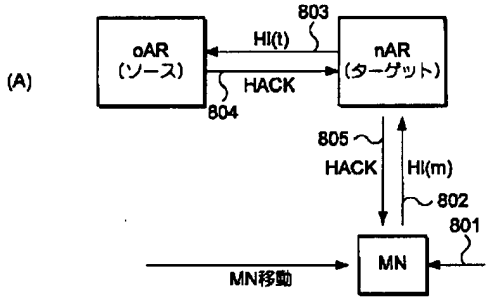
【図6】

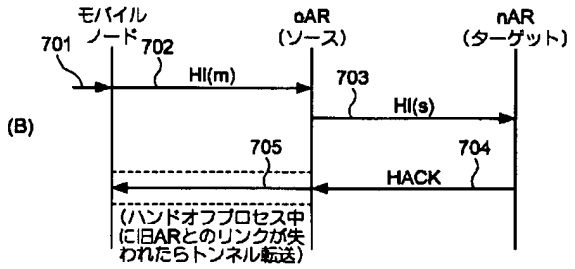
タイプ(8)	H	N	R	M	G	T	B	X	生存期間(16)
MNホームアドレス(32)									
HAアドレス(32)									
識別子(64)									
拡張...									

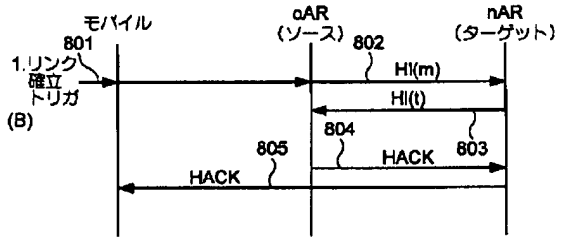
【図7】



【図8】







【図9】

タイプ	コード	チェックサム						
識別子		S	U	H	T	R	M	予約
オプション...								

【図10】

タイプ	コード	チェックサム					
識別子		S	U	H	T	R	予約
オプション...							

【図11】

タイプ	コード	チェックサム				
識別子		S	U	H	T	予約
オプション...						

フロントページの続き

(72)発明者　ヨングジュン　エル　グオン
アメリカ合衆国、カリフォルニア州
95110、サンノゼ、スイート300、メトロ
ドライブ181
(72)発明者　ジェームス　ケンプ
アメリカ合衆国、カリフォルニア州
95110、サンノゼ、スイート300、メトロ
ドライブ181
(72)発明者　フナト　ダイチ
アメリカ合衆国、カリフォルニア州
95110、サンノゼ、スイート300、メトロ
ドライブ181
(72)発明者　タケシタ　アツシ
アメリカ合衆国、カリフォルニア州
95110、サンノゼ、スイート300、メトロ
ドライブ181

Fターム(参考)　5K030 HA08 HC09 JL01
5K067 AA14 AA22 BB04 BB21 CC10
DD19 DD34 DD36 DD51 EE02
EE10 EE16 EE24 JJ39